DEPARTMENT OF HOMELAND SECURITY
UNITED STATES SECRET SERVICE
WASHINGTON, D.C. 20223

Freedom of Information Act & Privacy Act Program
Communications Center
245 Murray Lane, S.W., Building T-5
Washington, D.C. 20223

Date: FEB 15 2019

Jason Leopold
Senior Investigative Reporter
BuzzFeed News
[redacted]

File Number: 20171065

Dear Requester:

This is the final response to your Freedom of Information Act (FOIA) request, originally received by the United States Secret Service (Secret Service) on February 23, 2017, for information pertaining to all congressional correspondence (letters) from calendar year 2017 to date. Specifically, you are requesting, all letter correspondence sent by the agency to a congressional office, committee, subcommittee, chairman, ranking members, etc. Additionally, you are also requesting all letter correspondence sent to an agency by a Hill office.

Enclosed are documents responsive to your request. In an effort to provide you with the greatest degree of access authorized by law, we have considered this material under the FOIA statute, Title 5 U.S.C. § 552. Pursuant to this Act, exemptions have been applied where deemed appropriate. The exemptions cited are marked below.

In addition, approximately 210 page(s) were released, and approximately 41 page(s) were withheld in their entirety. An enclosure to this letter explains the exemptions in more detail.

☒ If this box is checked, deletions were made pursuant to the exemptions indicated below.

Section 552 (FOIA)

☐ (b) (1)	☐ (b) (2)	☐ (b) (3) Statute:		
☐ (b) (4)	☐ (b) (5)	☒ (b) (6)	☐ (b) (7) (A)	☐ (b) (7) (B)
☒ (b) (7) (C)	☐ (b) (7) (D)	☒ (b) (7) (E)	☐ (b) (7) (F)	☐ (b) (8)

The following checked item(s) also apply to your request:

☐ Some documents originated with another government agency(s). These documents were referred to that agency(s) for review and direct response to you.

☒ Some documents, in our files, contain information furnished to the Secret Service by another government agency(s). These documents were referred to that agency(s) for review and direct response to you.

☒ Fees: In the processing of this FOIA request, no fees are being assessed.

☐ Other:

If you deem our decision an adverse determination, you may exercise your appeal rights. Should you wish to file an administrative appeal, your appeal should be made in writing and received within ninety (90) days of the date of this letter, by writing to: Freedom of Information Appeal, Deputy Director, U.S. Secret Service, Communications Center, 245 Murray Lane, S.W., Building T-5, Washington, D.C. 20223. If you choose to file an administrative appeal, please explain the basis of your appeal and reference the case number listed above.

Additionally, you have the right to seek dispute resolution services from the Office of Government Information Services (OGIS) which mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Please note that contacting the Secret Service's FOIA Program and/or OGIS **is not** an alternative to filing an administrative appeal and **does not** stop the 90-day appeal clock. You may contact OGIS at: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001. You may also reach OGIS via e-mail at ogis@nara.gov, telephone at 202-741-5770/toll free at (877) 684-6448, or facsimile at (202) 741-5769.

If you need any further assistance, or would like to discuss any aspect of your request, please contact our FOIA Public Liaison Kevin Tyrrell, at (202) 406-6370. Alternatively, you may send an e-mail to foia@usss.dhs.gov.

FOIA/PA File No. 20171065 is assigned to your request. Please refer to this file number in all future communication with this office.

Sincerely,

Kim E. Campbell
Special Agent In Charge
Freedom of Information Act & Privacy Act Officer

Enclosure:
☒ FOIA and Privacy Act Exemption List

FREEDOM OF INFORMATION ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

Provisions of the Freedom of Information Act do not apply to matter that are:

(b) (1) (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(b) (2) related solely to the internal personnel rules and practices any agency;

(b) (3) specifically exempted from disclosure by statute (other than section 552b of this title), if that statute: (A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and (B) is established after the date of enactment of the OPEN FOIA Act of 2009;

(b) (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b) (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency; provided that the deliberative process privilege shall not apply to records created 25 years or more before the date on which the records were requested;

(b) (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b) (7) records or information compiled for law enforcement purposes, but only to the extent that the information: (A) could reasonable be expected to interfere with enforcement proceedings; (B) would deprive a person of a right to a fair trial or an impartial adjudication; (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (D) could reasonable be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source; (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b) (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for regulation or supervision of financial institutions;

(b) (9) geological and geophysical information and data, including maps, concerning wells.

PRIVACY ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

The provisions of the Privacy Act do not apply to:

(d) (5) material compiled in reasonable anticipation of civil action or proceeding;

(j) (2) material reporting investigative efforts pertaining to enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) material is currently and properly classified pursuant to an Executive Order in the interest of national defense or foreign policy;

(k) (2) material compiled during investigations for law enforcement purposes;

(k) (3) material maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;

(k) (5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or for access to classified information, but only to the extent that the disclosure of such material would reveal the identity of the person who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or prior to the September 27, 1975, under an implied promise that the identity of the source would be held in confidence;

(k) (6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process;

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE

DIRECTOR

Washington, D.C. 20223

February 16, 2017

The Honorable Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed you will find the U.S. Secret Service responses to your letter of February 6, 2017. If you or your staff has any questions regarding the enclosed material, please do not hesitate to contact my Deputy Assistant Director for Congressional Affairs, R. Christopher Stanley, by email at (b)(6);(b)(7)(C) or by phone at (202) 406-5676.

Respectfully,

Joseph P. Clancy

Enclosure

CC: The Honorable Claire McCaskill
Ranking Member

U.S. Secret Service Response to Senator Johnson's February 6, 2017 Letter

1. **Did the SAIC make any of the reported social media posts while on duty or using federal resources? Please explain.**

(b)(6);(b)(7)(C)

2. **What is the status of the USSS's investigation into this matter? Please explain.**

(b)(6);(b)(7)(C)

3. **Please provide a timeline for when USSS management learned of the SAIC's alleged social media posts. What actions did [the Secret Service] take when it received these allegations. Please explain.**

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

4. **When did the USSS receive allegations from the DHS OIG regarding the SAIC's alleged social media posts? What action did it take when it received these allegations? Please explain.**

   Please see response to question 3.

5. **Since the USSS became aware of the SAIC's social media posts, have her job duties been subject to review pending investigation. Please explain.**

   Yes, please see response to question 3 above for further detail.

6. **Has this matter been referred to the Office of Special Counsel? If so, when? If not, why?**

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

7. Please explain USSS's reasons for placing the SAIC on paid administrative leave.

(b)(6);(b)(7)(C)

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510–6250

February 6, 2017

The Honorable Joseph P. Clancy
Director
United States Secret Service
950 H Street, NW
Washington, DC 20223

Dear Director Clancy:

The Committee on Homeland Security and Governmental Affairs is examining social media statements allegedly made by the Special Agent-in-Charge (SAIC) of the United States Secret Service (USSS) field office in Denver, Colorado. I appreciate your assistance with this matter.

According to media reports, the SAIC reportedly wrote on Facebook in October 2016 about the presidential election. "As a public servant for nearly 23 years, I struggle to not violate the Hatch Act," she wrote. "To do otherwise can be a criminal offense for those in my position. Despite the fact that I am expected to take a bullet for both sides. But this world has changed and I have changed. And I would take jail time over a bullet or an endorsement for what I believe to be disaster to this country and the strong and amazing women and minorities who reside here. Hatch Act be damned. I am with Her."[1]

According to the Department of Homeland Security Office of Inspector General (DHS OIG), the OIG received a complaint about the SAIC's social media use in "mid-October" 2016 and referred the matter to USSS.[2] After recent media reports, the OIG reportedly received a second complaint, which it also referred to USSS.[3] In January 2017, USSS reportedly placed the SAIC on paid administrative leave.[4]

I fully support the right of all federal employees to engage in the political process, provided they follow the appropriate laws. Under the Hatch Act, USSS employees are subject to enhanced prohibitions on political activity that do not ordinarily apply to other federal

---

[1] *E.g.* (b)(6);(b)(7)(C) *Senior Secret Service agent suggests she wouldn't take 'a bullet' for Trump,* WASH. EXAMINER (Jan. 24, 2017), *available at* http://www.washingtonexaminer.com/senior-secret-service-agent-suggests-she-wouldnt-take-a-bullet-for-trump/article/2612814.

(b)(6);(b)(7)(C)

[2] Email from DHS OIG Staff to Comm. Staff, Jan. 27, 2017.

[3] *Id.*

[4] [redacted] *Secret Service puts agent who decried taking 'a bullet' for Trump on paid leave,* WASH. EXAMINER (Jan. 27, 2017), *available at* http://www.washingtonexaminer.com/secret-service-puts-agent-who-decried-taking-a-bullet-for-trump-on-paid-leave/article/2613210.

government employees.[5] To better understand the circumstances of these social media posts and USSS's response to them, I request the following information and materials:

1. Did the SAIC make any of the reported social media posts while on duty or using federal resources? Please explain.

2. What is the status of USSS's investigation into this matter? Please explain.

3. Please provide a timeline of when USSS management learned of the SAIC's alleged social media posts. What actions did USSS management take when made aware? Please explain.

4. When did USSS receive allegations from the DHS OIG regarding the SAIC's alleged social media posts? What action did it take when it received these allegations? Please explain.

5. Since USSS became aware of the SAIC's social media posts, have her job duties been subject to review pending investigation? Please explain.

6. Has this matter been referred to the Office of Special Counsel? If so, when? If not, why not?

7. Please explain USSS's reasons for placing the SAIC on paid administrative leave.

Please provide this information as soon as possible, but no later than 5:00 p.m. on February 20, 2017. In addition to a written response, I ask that your staff coordinate a staff-level briefing with Committee staff with respect to this matter. Please schedule this briefing by February 13, 2017.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency and economy of operations of all branches of the Government."[6] Additionally, S. Res. 73 (114th Congress) authorize the Committee to examine "the efficiency and economy of all branches and functions of Government with particular references to the operations and management of Federal regulatory policies and programs."[7]

If you have any questions regarding this letter, please ask your staff to contact (b)(6),(b)(7)(C) of the Committee staff at (b)(6),(b)(7)(C). Thank you for your prompt attention to this matter.

[5] 5 U.S.C. § 7323. Office of Special Counsel, *The Hatch Act: Permitted and Prohibited Activities for Federal Employees Subject to Further Restrictions*, Feb. 2016, *available at* https://osc.gov/Resources/HA%20Poster%20Further%20Restricted%202016.pdf.
[6] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[7] S. Res. 73 § 12, 114th Cong. (2015).

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Claire McCaskill
Ranking Member

The Honorable John Roth
Inspector General
U.S. Department of Homeland Security

The Honorable Carolyn Lerner
Special Counsel
U.S. Office of Special Counsel

Enclosure

Instructions for Responding to a Committee Request
Committee on Homeland Security and Governmental Affairs
United States Senate
115th Congress

A. Responding to a Request for Documents

1. In complying with the Committee's request, produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data, or information should not be destroyed, modified, removed, transferred, or otherwise made inaccessible to the Committee.

2. In the event that any entity, organization, or person denoted in the request has been or is also known by any other name or alias than herein denoted, the request should be read also to include the alternative identification.

3. The Committee's preference is to receive documents in electronic form (i.e. CD, memory stick, or thumb drive) in lieu of paper productions.

4. Documents produced in electronic form should be organized, identified, and indexed electronically.

5. Electronic document productions should be prepared according to the following standards:

    a. The production should consist of single page Tagged Image Files (".tif"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.

    b. Document numbers in the load file should match document Bates numbers and .tif file names.

    c. If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.

    d. All electronic documents produced should include the following fields of metadata specific to each document:

    BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD, INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION, BEGATTACH.

e. Alternatively, if the production cannot be made in .tif format, all documents derived from word processing programs, email applications, instant message logs, spreadsheets, and wherever else practicable should be produced in text searchable Portable Document Format (".pdf") format. Spreadsheets should also be provided in their native form. Audio and video files should be produced in their native format, although picture files associated with email or word processing programs should be produced in .pdf format along with the document it is contained in or to which it is attached. In such circumstances, consult with Committee staff prior to production of the requested documents.

f. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), consult with the Committee staff to determine the appropriate format in which to produce the information.

6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to the request should be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.

8. When producing documents, identify the paragraph in the Committee's schedule to which the documents respond.

9. Do not refuse to produce documents on the basis that any other person or entity also possesses non-identical or identical copies of the same documents.

10. This request is continuing in nature and applies to any newly discovered information. Any record, document, compilation of data or information not produced because it has not been located or discovered by the return date, should be produced immediately upon subsequent location or discovery.

11. All documents should be Bates-stamped sequentially and produced sequentially. Each page should bear a unique Bates number.

12. Two sets of documents should be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets should be delivered to the Majority Staff in Room 340 of the Dirksen Senate Office Building and the Minority Staff in Room 346 of the Dirksen Senate Office Building.

13. If compliance with the request cannot be made in full by the date specified in the request, compliance should be made to the extent possible by that date. Notify Committee staff as

soon as possible if full compliance cannot be made by the date specified in the request, and provide an explanation for why full compliance is not possible by that date.

14. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author, and addressee; and (e) the relationship of the author and addressee to each other.

15. In the event that a portion of a document is redacted on the basis of privilege, provide a privilege log containing the following information concerning any such redaction: (a) the privilege asserted; (b) the location of the redaction in the document; (c) the general subject matter of the redacted material; (d) the date, author, and addressee of the document, if not readily apparent; and (e) the relationship of the author and addressee to each other.

16. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.

17. If a date, name, title, or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date, name, title, or other descriptive detail is known to you or is otherwise apparent from the context of the request, produce all documents which would be responsive as if the date, name, title, or other descriptive detail was correct.

18. In the event a complete response requires the production of classified information, provide as much information in unclassified form as possible in your response and send all classified information under separate cover via the Office of Senate Security.

19. Unless otherwise specified, the period covered by this request is from January 1, 2009 to the present.

20. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

B. Responding to Interrogatories or a Request for Information

1. In complying with the Committee's request, answer truthfully and completely. Persons that knowingly provide false testimony could be subject to criminal prosecution for perjury (when under oath) or for making false statements. Persons that knowingly withhold subpoenaed information could be subject to proceedings for contempt of Congress. If you are unable to answer an interrogatory or information request fully, provide as much information as possible and explain why your answer is incomplete.

Instructions for Responding to a Committee Request

2. In the event that any entity, organization, or person denoted in the request has been or is also known by any other name or alias than herein denoted, the request should also be read to include the alternative identification.

3. Your response to the Committee's interrogatories or information requests should be made in writing and should be signed by you, your counsel, or a duly authorized designee.

4. When responding to interrogatories or information requests, respond to each paragraph in the Committee's schedule separately. Clearly identify the paragraph in the Committee's schedule to which the information responds.

5. Where knowledge, information, or facts are requested, the request encompasses knowledge, information or facts in your possession, custody, or control, or in the possession, custody, or control of your staff, agents, employees, representatives, and any other person who has possession, custody, or control of your proprietary knowledge, information, or facts.

6. Do not refuse to provide knowledge, information, or facts on the basis that any other person or entity also possesses the same knowledge, information, or facts.

7. The request is continuing in nature and applies to any newly discovered knowledge, information, or facts. Any knowledge, information, or facts not provided because it was not known by the return date, should be provided immediately upon subsequent discovery.

8. Two sets of responses should be delivered, one set to the Majority Staff and one set to the Minority Staff. When responses are provided to the Committee, copies should be delivered to the Majority Staff in Room 340 of the Dirksen Senate Office Building and the Minority Staff in Room 346 of the Dirksen Senate Office Building.

9. If compliance with the request cannot be made in full by the date specified in the request, compliance should be made to the extent possible by that date. Notify Committee staff as soon as possible if full compliance cannot be made by the date specified in the request, and provide an explanation for why full compliance is not possible by that date.

10. In the event that knowledge, information, or facts are withheld on the basis of privilege, provide a privilege log containing the following information: (a) the privilege asserted; (b) the general subject matter of the knowledge, information, or facts withheld; (c) the source of the knowledge, information, or facts withheld; (d) the paragraph in the Committee's request to which the knowledge, information, or facts are responsive; and (e) each individual to whom the knowledge, information, or facts have been disclosed.

11. If a date, name, title, or other descriptive detail set forth in this request is inaccurate, but the actual date, name, title, or other descriptive detail is known to you or is otherwise apparent from the context of the request, provide the information that would be responsive as if the date, name, title, or other descriptive detail was correct.

12. In the event a complete response requires the transmission of classified information, provide as much information in unclassified form as possible in your response directly to the Committee offices and send only the classified information under separate cover via the Office of Senate Security.

13. Unless otherwise specified, the period covered by this request is from January 1, 2009 to the present.

C. Definitions

1. The term "document" in the request or the instructions means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra- office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape, or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

2. The term "communication" in the request or the instructions means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether face to face, in meetings, by telephone, mail, telex, facsimile, email (desktop or mobile device), computer, text message, instant message, MMS or SMS message, regular mail, discussions, releases, delivery, or otherwise.

3. The terms "and" and "or" in the request or the instructions should be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.

Instructions for Responding to a Committee Request

4. The terms "person" or "persons" in the request or the instructions mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, businesses or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term "identify" in the request or the instructions, when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address, email address, and phone number.

6. The terms "referring" or "relating" in the request or the instructions, when used separately or collectively, with respect to any given subject, mean anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.

7. The term "employee" in the request or the instructions means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint venturer, loaned employee, part-time employee, permanent employee, provisional employee, or subcontractor.

8. The terms "you" and "your" in the request or the instructions refer to yourself; your firm, corporation, partnership, association, department, or other legal or government entity, including all subsidiaries, divisions, branches, or other units thereof; and all members, officers, employees, agents, contractors, and all other individuals acting or purporting to act on your behalf, including all present and former members, officers, employees, agents, contractors, and all other individuals exercising or purporting to exercise discretion, make policy, and/or decisions.

# # #

MICHAEL T. McCAUL, TEXAS
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
Ranking Member

One Hundred Fifteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington DC 20515

January 9, 2017

Mr. Joseph P. Clancy
Director
United States Secret Service
Washington, D.C. 20223

Dear Director Clancy,

The U.S. Secret Service (USSS) carries out a combined, integrated mission of protecting the President and other dignitaries and also investigating and preventing a variety of financial and electronic crimes. To effectively carry out these dual responsibilities, the USSS initiated the Information Integration Technology Transformation (IITT) program to modernize the information technology (IT) systems used to support its functions.

We have had concerns about USSS oversight of IT programs and the security of those systems more broadly. In November 2015, our Oversight and Management Efficiency Subcommittee held a hearing examining challenges related to USSS employees improperly accessing and distributing personally identifiable information to other employees.[1] In that hearing, you reassured us that employee access to sensitive information had been limited based on job functions due to progress made in decommissioning legacy IT systems and, among other things, implementing IITT.

However, in October 2016, the Department of Homeland Security's (DHS) Office of Inspector General (OIG) reported that the USSS's management of its IT systems was ineffective, in part, due to a lack of priority focus by management.[2] In particular, the OIG reported that the USSS's Chief Information Officer (CIO) did not have authority over all IT investments and did not provide adequate attention to IT policies. In addition, the OIG reported that several key IT systems had expired authorities to operate (ATO).[3] As you know, without ATOs, the OIG concluded that USSS cannot adequately safeguard its systems. Further, the OIG found that the CIO's office struggled with vacancies in key positions, which further corroded management of IT systems.

---

[1] House Homeland Security Committee, Subcommittee on Oversight and Management Efficiency, *Examining Ongoing Challenges at the U.S. Secret Service and Their Governmentwide Implications* (Washington, D.C.: Nov. 17, 2015).
[2] DHS OIG, *USSS Faces Challenges Protecting Sensitive Case Management Systems and Data,* (Washington, D.C.: Oct. 7, 2016).
[3] ATOs are certifications by the CIO that certain IT security controls are in place, as required by DHS policy (*DHS Sensitive Systems Policy Directive 4300A).*

On October 18, 2016, Committee staff met with the USSS CIO who told them that 75% of the U.S. Secret Service's IT systems had ATOs and all IT systems would have ATOs by December 31, 2016. However, we have heard reports that, near the time of that briefing, the actual number of USSS IT systems with ATOs was significantly less than Committee staff were told. In addition to this discrepancy, in November 2016, the USSS CIO testified before a House of Representative's oversight committee that the component had rectified "all" issues identified in the OIG report and implemented many of the OIG's 11 recommendations.[4] However, according to the OIG, the USSS has not provided adequate information to close out any of these recommendations and, fundamentally, has not ensured that all IT systems are secure by having valid ATOs.

Given the challenges identified by the OIG and the discrepancies in information outlined above, we request that the USSS provide the following information by January 27, 2017, pursuant to Rule X(3)(g) of the Rules of the House of Representatives:

1. The number of USSS IT systems with current ATOs.
2. The number of USSS IT systems with current ATOs certified by the current CIO.
3. The total number of USSS IT systems.
4. If USSS IT systems do not have current ATOs, a proposed timeline and steps the USSS plans to take to ensure that all IT systems without ATOs are certified.
5. Actions taken to implement recommendations from the OIG's October 2016 report.
6. Within OCIO, the number of currently vacant positions, the number of positions to be filled this fiscal year, and the total number of authorized positions in OCIO this fiscal year.
7. Information on the USSS's strategy for filling remaining vacant OCIO positions and anticipated challenges in being unable to do so.

We look forward to hearing from you regarding this request. Should you have any questions on this request, please contact (b)(6);(b)(7)(C) and (b)(6);(b)(7)(C) of the majority staff at (b)(6);(b)(7)(C) and (b)(6);(b)(7)(C) of the minority staff at (b)(6);(b)(7)(C)

Respectfully,

MICHAEL T. McCAUL
Chairman

BENNIE G. THOMPSON
Ranking Member

[4] *Oversight of the Secret Service*, House Committee on Oversight and Government Reform (Washington, D.C.: Nov. 15, 2016).

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE

DIRECTOR

Washington, D.C. 20223

January 30, 2017

The Honorable Michael McCaul, Chairman
Committee on Homeland Security
2001 Rayburn House Office Building
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Bennie Thompson, Ranking Member
Committee on Homeland Security
2466 Rayburn House Office Building
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman McCaul and Ranking Member Thompson:

I sincerely appreciate the Committee's continued interest in the U.S. Secret Service's (Secret Service) efforts to modernize the information technology (IT) systems. I firmly believe that robust information security and a modern IT infrastructure are foundational to the success of the Secret Service mission. Since the Information Integration and Technology Transformation (IITT) program began with funding in 2010, significant strides have been made to provide secure capabilities to a highly mobile workforce.

As your letter of January 9, 2017 states, during a Congressional hearing on November 15, 2016, Chief Information Officer (CIO) Kevin Nally provided testimony regarding the state of the Secret Service's information technology systems, as well as our progress toward addressing the recommendations from the Department of Homeland Security (DHS) Office of Inspector General (OIG) report titled "USSS Faces Challenges Protecting Sensitive Case Management Systems and Data."

CIO Nally testified that the Secret Service made significant progress implementing the DHS OIG's recommendations, and stated that, "all this has been rectified" and that six of the seven recommendations that fall within his purview were closed. While OIG recommendations are categorized as unresolved or resolved, and open or closed, it was my understanding that the CIO was speaking from an operational perspective, rather than using OIG terminology. At the time, all of the recommendations in the report were considered resolved and open.

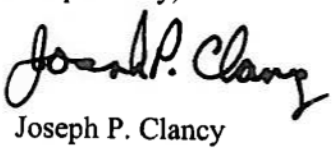
As is standard procedure, we provided updates on our progress to the OIG on January 4, 2017, in the required 90-day update document. In addition to the formal letter detailing the work completed and the steps we have taken, we also provided the OIG with documentation intended to demonstrate the work accomplished and officially close with the OIG eight of the open-resolved recommendations. It is understandable that Inspector General Roth disagreed with CIO Nally's testimony in his letter dated November 28, 2016. Until the first week of January, his

office had not seen any of the documentation showing the work we had done and would have considered the recommendations open.

My hope is that this letter, and the accompanying enclosure, clarifies the direction and progress that is being made with regard to the Secret Service information technology systems. We appreciate the OIG's audit on our IT systems and recognize that continued improvements are needed and essential to the successful completion of our mission. The Secret Service will continue to improve the oversight and management of our IT systems to ensure that the information with which it is entrusted is properly protected and secured.

If you or your staff has any questions regarding the enclosed material, please do not hesitate to contact my Deputy Assistant Director for Congressional Affairs, Chris Stanley, by email at (b)(6);(b)(7)(C) or by phone at (202) 406-5676.

Respectfully,



Joseph P. Clancy

Enclosure

U.S. Secret Service Response to
Committee on Homeland Security Letter dated January 9, 2017

1. The number of USSS IT systems with current ATOs.
   Response: There are nine IT systems with current ATOs.

2. The number of USSS IT systems with current ATOs certified by the current CIO.
   Response: There are nine IT systems with current ATOs certified by the current CIO.

3. The total number of USSS IT systems.
   Response: The Secret Service has twenty-one operational IT systems.

4. If USSS IT systems do not have current ATOs, a proposed timeline and steps the USSS plans to take to ensure that all IT systems without ATOs are certified.
   Response: Please see the proposed timeline on systems without ATOs below:

(b)(7)(E)

5. Actions taken to implement recommendations from the OIG's October 2016 report.
   Response: Please see Attachment A.

6. Within OCIO, the number of currently vacant positions, the number of positions to be filled this fiscal year, and the total number of authorized positions in OCIO this fiscal year.
   Response: Please see recommendation 9 in Attachment A.
7. Information on the USSS's strategy for filling remaining vacant OCIO positions and anticipated challenges in being unable to do so.
   Response: Please see recommendation 9 in Attachment A.

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE
Washington, D.C. 20223

January 4, 2017

MEMORANDUM FOR: Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits
Office of the Inspector General
U.S. Department of Homeland Security

FROM: Percy L. Howard, Jr.
Assistant Director
Office of Professional Responsibility
U.S. Secret Service

SUBJECT: 90 day update on OIG Report: "USSS Faces Challenges Protecting Sensitive Case Management Systems and Data" (OIG 17-01)

In accordance with the Department of Homeland Security Directive 077-01-001, this memorandum provides updates on Secret Service actions to address the OIG's recommendations.

In our original response, we concurred with OIG recommendations 1-10 and the Department of Homeland Security (DHS) Privacy Office (PRIV) concurred with the eleventh recommendation. We are currently requesting closure of eight open-resolved recommendations.

Please find our original detailed response to each recommendation as well as an update on our progress attached. Where noted, additional documents will be sent separately.

Attachment

RIF

LOIS FRANKEL
21ST DISTRICT, FLORIDA

WASHINGTON OFFICE
1037 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-9890

DISTRICT OFFICE
2500 NORTH MILITARY TRAIL
SUITE #490
BOCA RATON, FL 33431
(561) 998-9045
TOLL FREE (866) 264-0957

frankel.house.gov

Congress of the United States
House of Representatives
Washington, DC 20515–0921

COMMITTEE ON FOREIGN AFFAIRS

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

CO-CHAIR CONGRESSIONAL CAUCUS FOR WOMEN'S ISSUES

STEERING AND POLICY COMMITTEE

January 24, 2017

The Honorable Joseph P. Clancy
Director
United States Secret Service
245 Murray Lane
Washington, DC 20223

Dear Director Clancy:

I would like to respectfully request a meeting or phone call with you or your designee to discuss security-related flight restrictions in Palm Beach County, Florida.

(b)(7)(E)

These restrictions could hurt a number of local businesses. For example, Palm Beach Aircraft Services Inc. reported to the Sun Sentinel that the organization estimates it will lose two million dollars in revenue each year as a direct consequence of these restrictions. In addition, Palm Beach Flight Training at Lantana Airport could be put entirely out of business.

I look forward to discussing these issues with you or your staff. Should you have questions or concerns, please contact my Chief of Staff, (b)(6);(b)(7)(C) at (b)(6);(b)(7)(C)

Sincerely,

Lois Frankel
Member of Congress

MICHAEL T. McCAUL, TEXAS
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Fifteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

January 25, 2017

Mr. Joseph P. Clancy
Director
United States Secret Service
Department of Homeland Security
Washington, D.C. 20528

Dear Director Clancy:

I would like to congratulate The United States Secret Service (USSS) on ensuring a peaceful transition of power at the recent Inauguration ceremonies and accompanying events. As always, the agency performed impeccably well by protecting our nation's leaders and those visiting Washington throughout Inauguration weekend. In 2016, the USSS demonstrated its commitment to excellence while managing security for a number of National Special Security Events, as well as a high profile presidential campaign cycle. I applaud your leadership and the men and women of your agency for steadfastly performing your mission, and I look forward to working with you as we enter a new Administration and the 115th Congress.

Additionally, I would like to express concern for recent media reporting surrounding the social media posts of a high-ranking Secret Service agent, Ms. Kerry O'Grady, who has been serving as the special agent in charge of the USSS Denver field office. According to a recent media report, in October of last year, Ms. O'Grady made overtly political posts to her Facebook account, while also suggesting that she would willfully violate the Hatch Act. Moreover, she made a concerning suggestion that she would refuse to fulfil her protective duties for the President of the United States, due to her personal political views.[1] While I have complete confidence in the Secret Service to fulfil its protective mission, Ms. O'Grady's comments were wholly inappropriate for any USSS agent, particularly one of such high stature in the agency.

---

[1] (b)(6);(b)(7)(C) "Senior Secret Service Agent Suggests She Wouldn't Take a Bullet for Trump," *Washington Examiner*, January 24, 2017 < http://www.washingtonexaminer.com/senior-secret-service-agent-suggests-she-wouldnt-take-a-bullet-for-trump/article/2612814>.

Because of this, I would like to express my hope that you will ensure a thorough investigation into this matter and request a response to the following questions by January 31, 2017:

1. What are the policies governing social media activity by employees of the USSS?
2. How does the Secret Service investigate and adjudicate reported violations of either agency policy or the Hatch Act?
3. How many such violations have occurred in the last three fiscal years?
4. What training is provided to USSS employees regarding social media use?
5. Does the USSS have any policies requiring prior agency approval when an employee issues comments to the press?
6. Typically, what are the penalties for violations of social media policies and the Hatch Act?
7. When did the agency first become aware of Ms. O'Grady's comments?
8. How does the Secret Service plan to investigate Ms. O'Grady's case?

The men and women of the USSS are among the finest, most capable agents and officers in the world, and their mission is of the utmost importance to the national security of the United States. However, incidents such as this only serve to further harm morale within the agency, and it is my intention to work with you to improve morale and enhance the overall standing of the Secret Service. With this in mind, I look forward to a continuing and open dialogue with you.

Thank you for your prompt attention to this matter. Should you have any questions please reach out to Ms. (b)(6);(b)(7)(C) on the Committee staff at (b)(6);(b)(7)(C).

Sincerely,

John Katko
Chairman
Subcommittee on Transportation
and Protective Security

DIRECTOR

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE
Washington, D.C. 20223

February 2, 2017

The Honorable John Katko
Chairman
Subcommittee on Transportation & Protective Security
Committee on Homeland Security
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed you will find the U.S. Secret Service responses to your letter of January 25, 2017. If you or your staff has any questions regarding the enclosed material, please do not hesitate to contact my Deputy Assistant Director for Congressional Affairs, R. Christopher Stanley, by email at (b)(6);(b)(7)(C) or by phone at (202) 406-5676.

Respectfully,

Joseph P. Clancy

Enclosure

U.S. Secret Service Response
to Committee on Homeland Security Subcommittee on Transportation & Protective Security
letter dated January 25, 2017

1. **What are the policies governing social media activity by employees of the USSS?**
A copy of the Office of Government Public Affairs Manual, Chapter PAF-08, and Social Media (PAF-08 (01) through PAF-08 (07) is enclosed.

2. **How does the Secret Service investigate and adjudicate reported violation of:**
a. agency policy -
The Secret Service investigates reported violations of agency policy through its Office of Professional Responsibility (RES), Inspecton Division; and adjudicates those violations through its Office of Integrity in accordance with the provisions of title 5 of the United States Code (USC), Chapter 75, title 5 of the Code of Federal Regulations (CFR), Part 752, and Secret Service policy, Office of the Director Manual, section ITG-06(01) (copy enclosed).

b. the Hatch Act -
The Secret Service is prevented by law from investigating and adjudicating reported violations of the Hatch Act. Pursuant to 5 U.S.C., section 1216, 5 C.F.R., section 734.102(a), the Office of Special Counsel (OSC) has exclusive jursdiction to investigate and seek corrective action for alleged violations of the Hatch Act. The Merit Systems Protection Board (MSPB) has the exclusive authority under title 5, U.S.C., section 1204 and title 5, C.F.R., section 734.102(b), to determine whether a violation of the Hatch Act has occurred and to impose a penalty for a violation.

3. **How many such violations have occurred in the last three fiscal years?**
The Secret Service understands that "such violations" refers to violations of the Hatch Act or violations of Secret Service policy otherwise related to the use of social media (but not a Hatch Act violation). In regard to the Hatch Act, the Secret Service has referred three potential Hatch Act violations to the OSC within the last three fiscal years. In regard to one of the referrals, the OSC completed its investigation and reached agreement with the employee in regard to disciplinary action. The other two referrals remain under review by the OSC.

In regard to non-Hatch Act violations related to the use of social media, there has been one adjudicated violation in the past three fiscal years.

4. **What training is provided to USSS employees regarding social media use?**
The Secret Service Office of Chief Counsel provides annual Government ethics training to employees required to receive such training under the Ethics in Government Act. This training has included specific information in regard to the Hatch Act and the use of social media in that context. Additionally, on October 30, 2015, the Secret Service Office of Human Resources issued an Agency wide directive providing information concerning the Hatch Act and the related use of social media: on December 11, 2015, the Department of Homeland Security issued an employee wide communication concerning "Ethics Considerations During the Political Campaign Season" which provided information concerning the Hatch Act and the use of social media: and on July 13, 2016, the Secret

Service Office Office of Chief Counsel issued to all employees, a memorandum titled "Hatch Act Guidance – Employees at Conventions," again providing information concerning the Hatch Act and the use of social media. Further, the Hatch Act prohibitions are discussed in three Secret Service policies, the Office of the Director Manual, section ITG-03(08), the Government and Public Affairs Manual, section PAF 08(02), and the Office of Human Resources Manual, section HCD-05. Copies of these communications are enclosed.

The Secret Service also provides its employees with online training courses which touch or focus on various issues involving the use of social media. These include the following three courses. The first course titled "Social Engineering Prevention and Awareness Training," focuses on social engineering (cyber) attacks with an emphasis on phishing, spear phishing and whaling. The course includes some examples (named as Facebook and Twitter) where social media is used in phishing (hooks). The second course titled "Decision Making Elements (Ethics)," focuses on identifying the risks involved in employee decision making in regard to both work and personal life. This course is geared toward ensuring that an employee's actions do not lead to administrative and/or criminal ramifications. Scenarios in this course include an example of an employee posting on a family member's social media page during a local campaign. The third course titled "Operational Use of Social Media," is intended to address the allowable use of social media in an operational or investigative capacity. This course is targeted toward criminal law enforcement and protective intelligence personnel.

5. **Does the USSS have any policies requiring prior agency approval when an employee issues comments to the press?**
Yes, the Secret Service Media Policy, PAF-03, states that all media inquires and requests for interviews, without exception, must be referred to the appropriate Special Agent in Charge or Division Chief. Additionally, inquiries of national significance or from national media entities must be forwarded to the Office of Government and Public Affairs, Public Affairs Program, in our Washington, D.C. headquarters. A copy of PAF-03 is enclosed.

6. **Typically, what are the penalties for violations of:**
a. social media policies -
The Secret Service Table of Penalties, ITG-04, Offense Code 5.12, Failure to Follow Instructions, provides for a standard penalty of a three day suspension from duty, mitigated penalties of a letter of reprimand to a one day suspension, and aggravated penalties of a five to seven day suspension. Offense Code 5.35, Violation of Miscellaneous Rules/Regulations, provides for a standard penalty of a five day suspension, mitigated penalties of a letter of reprimand to a three day suspension, and aggravated penalties of a seven to a thirty day suspension. Depending on the seriousness of the violation, Offense Codes, 5.31 and 5.32, Unprofessional Conduct – Off Duty and Unprofessional Conduct – On Duty might apply to such a violation. Unprofessional Conduct – Off Duty, carries a standard penalty of a five day suspension, mitigated

penalties of a Letter of Reprimand to a three day suspension, and aggravated penalties of a seven day suspension to removal. Unprofessional Conduct – On Duty, carries a standard penalty of seven day suspension, mitigated penalties of a Letter of Reprimand to a five day suspension, and aggravated penalties of a ten day suspension to removal.

b. the Hatch Act -
Under title 5, U.S.C., section 1204 and title 5, C.F.R., section 734.102(b), the MSPB has exclusive authority to determine whether a violation of the Hatch Act has occurred and to impose a penalty of removal, reduction-in-grade, debarment from Federal employment for a period not to exceed 5 years, suspension, reprimand, or an assessment of a civil penalty not to exceed $1,000, for such violations.

7. **When did the Agency first become aware of Ms. O'Grady's comments?**
The Secret Service first became aware of Ms. O'Grady's original comments on November 17, 2016, when the Department of Homeland Security, Office of Inspector General, provided this information to the Secret Service's Office of Professional Responsibility.

8. **How does the Secret Service plan to investigate Ms. O'Grady's case?**
The Secret Service has contacted the OSC to determine if Ms. O'Grady's postings or other actions represent a potential Hatch Act violation and should be referred to that office for investigation and adjudication.

In regard to the remaining portions of Ms. O'Grady's case, after consideration, the DHS Office of Inspector General deffered the investigation to the Secret Service. RES is investigating that matter through a review of available information and a series of witness interviews. Once completed, the results of that investigation will be provided to the Secret Service's Intake Group for possible referral to the Office of Integrity for adjudication of any disciplinary action pursuant to federal statutes, regulation and agency policy. Further, as Ms. O'Grady holds a (b)(6);(b)(7)(C) the matter may also be referred to the Security Management Division for adjudication of any potential security violation.

CONTENT MANAGEMENT ON PUBLIC-FACING WEBSITES AND SOCIAL MEDIA

Purpose

This directive establishes Secret Service policy regarding the management of all Secret Service content posted on public-facing networks and social networking websites and applications. Content is information of any kind published to the web (including text, graphics, symbols, retrievable data, and presentation concepts).

Social media is characterized as the collection of web tools that facilitate collaboration and information sharing. Web-based communities and hosted services include social networking sites, video and photo sharing sites, wikis, blogs, virtual worlds, and other emerging technologies.

Refer to the Government and Public Affairs Manual section PAF-03, for public relations media policy.

Refer to the Technical Development and Mission Support Manual section OPSC-01, for United States Secret Service Operational Security Program (OPSEC) policy.

Refer to the Technical Development and Mission Support Manual, IRM chapter, for technical controls.

Refer to the Professional Responsibility Manual section MNO-6, for records management policy.

Scope

This directive applies to all Secret Service employees. It also applies to contractors engaged in social media on behalf of the Secret Service as part of their duties.

The scope of this directive is limited to the use and management of Secret Service web information and associated systems where the intent is to make information available to the public or to a general audience within the Department of Homeland Security (DHS or Department).

This directive does not apply to internal Secret Service activities (such as on Intranets, applications, or interactions that do not involve the public), or to activities that are part of authorized law enforcement, national security, or intelligence activities.

Definition of Terms

Refer to the Government and Public Affairs Manual section PAF-08(07), Glossary of Social Media Terms, for the definition of terms.

Background

Social media hosts are public, content sharing websites that allow individual users to upload, view, and share content such as video clips, press releases, opinions, and other information.

Social networking interactions and applications include a sphere of non-government websites and web-based tools that focus on connecting users, inside and outside of the DHS and Secret Service, to engage in dialogue, share information and media, and collaborate. Third-parties control and operate these non-governmental websites; however, the Department and the Secret Service may use them as alternative channels to provide information and engage with the public. The Department and the Secret Service may also use these websites to make information and services widely available, while promoting transparency and accountability, as a service for those seeking information about or services from the Secret Service.

In accordance with the President's Memorandum on Transparency and Open Government (January 21, 2009) and the Director of the Office of Management and Budget's (OMB) Open Government Directive Memorandum (December 8, 2009), the Department and the Secret Service may utilize the opportunity that social networking presents to provide the public with robust information through many channels and to further engage the public.

While these collaborative tools present many useful opportunities, their application must not compromise data confidentiality and integrity.

Responsibilities

Assistant Director of Government and Public Affairs (GPA): The Assistant Director of Government and Public Affairs or designee shall be responsible for the implementation of this directive.

Special Agent in Charge (SAIC), Public Affairs Program, GPA: The SAIC, Public Affairs Program, serves as the Secret Service's central point of contact for posting content to social media and public-facing websites. The SAIC of Public Affairs shall:

- Ensure that style, message, and content on the Internet conform to the direction and vision set by the Director;
- Provide and publish content describing the Secret Service's mission, statutory authority, organization structure, and Strategic Plan as required by the E-Government Act of 2002, as amended;
- Ensure that website initiatives adhere to policies, laws, regulations, and guidance including those regarding accessibility, privacy, security, and records management;
- Establish a formal process for publishing information to the web that accommodates the requirements of this directive and applicable authorities;
- Develop and maintain content for the Secret Service web presence;
- Respond to certification and reporting requirements for Secret Service web information and associated systems; and

- Designate a web content manager.

Chief Counsel: The Office of Chief Counsel provides advice and assistance on all legal matters arising out of, or incident to, the use of social media.

Disclosure Officer: The Disclosure Officer is the privacy point of contact for the Secret Service. The Disclosure Officer is responsible for privacy compliance across the Secret Service, including assuring that technologies used by the Secret Service sustain and do not erode privacy protections relating to the use of personal and Secret Service information.

The Disclosure Officer is responsible for compliance with Federal laws and DHS privacy policy at the Secret Service level. The Disclosure Officer works with the Secret Service Chief Information Officer (CIO) and DHS Chief Privacy Officer (CPO) to maintain privacy requirements.

Chief Records Officer (CRO): Management and Organization Division's (MNO) Chief Records Officer is responsible for coordinating with and assisting the Public Affairs Program to ensure social media records are properly identified, managed, and handled in accordance with National Archives and Records Administration (NARA)-approved schedules, including any NARA-approved schedules specifically developed for social media content. MNO's Record Programs Management Branch shall provide proper records management retention guidance in accordance with NARA-approved record schedules, Freedom of Information Act (FOIA) requests, and e-discovery litigation holds.

Chief Information Officer (CIO): The Chief Information Officer shall:

- Provide overall policy implementation and procedural guidance for the web and associated systems;
- Ensure adherence to policies, laws, regulations, and guidance including those regarding accessibility, privacy, and security;
- Develop and maintain the System Security Plan for web-associated systems. (web-associated systems refer to those systems that comprise the Secret Service web and are not directly attributable to specific programs, such as web servers, gateways, security software and appliances and other ancillary components.);
- Establish and enforce technical standards;
- Authorize all Secret Service websites; and
- Provide technical procedural guidance for establishing and maintaining Secret Service websites.

Chief Information Security Officer (CISO): The Chief Information Security Officer within the CIO Program shall:

- Provide policy implementation and procedural guidance regarding information and information system security for the web;
- Ensure that Secret Service web information and associated systems adhere to laws, regulations, policies, and guidance regarding security; and
- Review and approve the System Security Plans for web-associated systems.

Content Managers: Web content managers shall:

- Review and approve web content within their area of responsibility;
- Manage web content incidents; and
- Ensure that web content within their area of responsibility adheres to laws, regulations, policies, and guidance including those regarding accessibility, privacy, and security.

All Employees and Contractors: All employees and contractors shall:

- Comply with this and other directives prescribing the use and management of web information and associated systems; and
- Report discrepancies or policy inconsistencies reflected in web content to appropriate managers.

Policy

1. Unless otherwise directed by statute, Executive Order, or regulation, Secret Service Public Affairs officials serve as the primary account holder for all social networking websites and applications across the Secret Service, and manage and approve all Secret Service content posted on public-facing websites. All content disseminated through official Secret Service accounts must be approved by Public Affairs officials prior to posting. Public Affairs officials will ensure that all posted content falls within the appropriate requirements for publicly available information and materials. Secret Service Public Affairs officials will, when necessary, act as the final authority on what content is acceptable for posting.

2. It is imperative that the Secret Service engage the public in a manner that complies with Federal accessibility, privacy, information security, and records laws. To ensure that the Secret Service's use of social media complies with Federal laws, Executive Orders, regulations, and policies, and to apply standards consistently across the entire Secret Service, the Office of the Chief Counsel, Equal Employment Opportunity (EEO) Program, Freedom of Information Act and Privacy Act Program, Public Affairs Program, Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Chief Records Officer (CRO) will collaborate to ensure that all activities related to social media are evaluated and that compliance issues are considered and coordinated before implementation.

3. Only GPA-designated content managers may post content, and only those individuals designated by GPA for this purpose shall be granted access on a continuing basis.

4. Employees' personal accounts shall not be used to convey official Secret Service communications.

5. As part of their official contractual duties, and only under close oversight by a Federal employee, contractors may provide support for Secret Service social media websites and applications. Any postings by a contractor must be specifically approved by Secret Service personnel.

6. The Office of Government and Public Affairs reserves the right to terminate a content manager's access to social media, or to terminate a social media tool at any time, within its sole discretion.

7. Wikis are a collection of web pages that encourage users to contribute or modify content. If Secret Service personnel believe there is a need to edit wiki content, concerns must be brought to the PAF

officials for discussion, including the pages in question and proposed modifications (such as erroneous information). If there is agreement by PAF of the need to edit, PAF staff will make the necessary changes. PAF staff editors must identify themselves as employees of the Secret Service on the pages. There should never be anonymous editing.

8. Posted content shall be in keeping with DHS's Terms of Service (TOS) and guidelines for a given social media host (e.g., YouTube, Twitter, etc.) This condition is also met if DHS endorses another appropriate Federal agency's guidance or TOS (e.g., General Services Administration, Office of Personnel Management). Under no circumstances shall sensitive information be posted to social media sites.

9. Content shall not be posted to any social media site for which the Secret Service has not approved and published final posting guidelines and TOS.

10. Content managers shall review and understand the appropriate DHS-level TOS for the appropriate social media host.

11. Content managers shall make a risk-based decision prior to posting any information and shall recognize that social media hosts are not DHS/Secret Service information systems and, therefore, subject only to the DHS TOS and not to DHS or Secret Service policy. Once released, information is no longer under DHS or Secret Service control.

12. Content managers shall follow DHS's "Department PDF Standards" to ensure hidden data has been removed from documents prior to posting them on the Internet. These standards are located on the DHS Online Web Center.

13. DHS has set forth specific requirements on how the Department and its components (e.g., Secret Service) may engage in social networking, including the use of applications in a privacy sensitive way. Refer to DHS's Privacy Impact Assessments (PIA) for the Use of Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue), and Use of Unidirectional Social Media Applications Communications and Outreach, which can be found at http://www.dhs.gov/privacy.

14. If the Secret Service has an operational need to use social networking interactions or applications that is outside the scope of the requirements and analytical understanding outlined in the DHS PIAs referenced above, a separate PIA must be written for the Secret Service's use of social networking interactions or applications to address the specific privacy concerns that are unique to that initiative for consideration by DHS's Chief Privacy Officer.

Content Management

1. The SAIC of PAF is responsible for establishing a formal process for determining what information to publish to the web. The process shall include review and approval measures to ensure compliance with all laws, regulations, policies, and guidance, including those regarding accessibility, privacy, and security.

2. Only official descriptions of Secret Service missions and entities shall be used on Secret Service Internet websites.

3. Secret Service websites shall have a mission orientation. A linkage between the content and Secret Service's strategic goals and objectives should be apparent.

4. Information shall only be published to the web by persons or entities that can rightfully be considered the controlling authority of the information.

5. All Secret Service websites and pages shall comply with DHS, Secret Service, and Government-wide policy regarding records management.

6. Managers of sites or pages that provide the ability to contact Secret Service with the expectation of a response shall ensure that a mechanism is in place to provide an accurate response within a reasonable timeframe – generally within three working days.

7. Links to pages outside of Secret Service websites are authorized in support of valid business objectives. Links may not endorse a particular non-Governmental product or service or provide preferential treatment. No payment of any kind shall be accepted to provide a link on any Secret Service web page to another web page or to provide specific content on a Secret Service web page. Refer to the Government and Public Affairs Manual section PAF-09(02), for policy addressing external links from Secret Service public-facing websites.

8. The following categories of information are prohibited on public-facing websites:

   - Classified information;
   - For Official Use Only (FOUO) information;
   - Official Use Only (OUO) information;
   - Law Enforcement Sensitive (LES) information;
   - Limited Official Use Only (LOUO) information;
   - Controlled Unclassified Information (CUI);
   - Inflammatory comments;
   - Information protected under the Privacy Act;
   - Advertisements or endorsements of commercial products or services;
   - Copyrighted or trademarked material without explicit permission from the author or not subject to fair use. "Fair use" is a legal concept that permits the use of copyrighted material within certain limitations, such as quoting a short excerpt of a publication. Only the Office of Chief Counsel shall make fair use determinations;
   - Personal statements regarding political candidates, politics, or other political statements;
   - Pornographic material;
   - Information regarding Secret Service personnel or their families;
   - Information that would interfere with an official investigation or law enforcement activity, or judicial proceeding, including information that could subject law enforcement personnel to potential harm;
   - Internal program agenda, correspondence, and memoranda not appropriate for general distribution;

- Pre-decisional information, reader files, internal letters, and memoranda shall not be released unless approved by the appropriate authority through the SAIC of Public Affairs;
- Procurement-sensitive or proprietary information;
- Personal opinion or private agenda;
- Duplication of DHS or Secret Service directives or other Government documents;
- Links from Secret Service Internet sites to Secret Service Intranet sites; and
- Operations Security (OPSEC) and Information Security (INFOSEC) material.

Privacy

1. The Disclosure Officer is the authority on privacy matters relating to web information and information systems.
2. All web information and associated systems shall comply with the Privacy Act of 1974 and other applicable laws, regulations, and privacy policies.
3. A standard privacy statement shall be applied Secret Service-wide and shall be readily accessible from all top level, or entry point Secret Service web pages. Refer to the Government and Public Affairs Manual section PAF-09(01), Posting Website Policies and Notices.
4. Information gathering, use, dissemination, and protection shall be in compliance with Government and Public Affairs Manual section LIA-03, Freedom of Information Act (FOIA) and Privacy Act.
5. No web page shall be used to gather information from the public or monitor public use of the Secret Service Internet without the express authority of the Secret Service Chief Information Officer (CIO).
6. Refer to the Government and Public Affairs Manual section PAF-08(04), Social Media and Privacy Issues, for additional information regarding privacy.

Accessibility

1. The CIO is the authority on accessibility matters relating to web information and associated systems for the Secret Service.
2. All web information and associated systems shall comply with Section 508 of the Rehabilitation Act of 1973, and all other applicable DHS and Secret Service specific and government-wide accessibility policies. Refer to the Technical Development and Mission Support Manual section IRM-02(06), IT Accessibility Review, for policy to ensure Section 508 compliance.

Records Management

When using electronic media, whether it is a blog, a website, a wiki, e-mail, or any other type of electronic communications, the regulations that govern proper management, and archiving of records, and release of information (Freedom of Information Act) still apply. Content managers, working with the MNO's Chief Records Officer, shall determine the most appropriate methods to capture and retain records on both Government servers and technologies hosted on non-Federal hosts. The National Archives and Records Administration and DHS offer resources and guidance to agencies to ensure proper records management. Secret Service records management directives are contained in the Professional Responsibility Manual, MNO chapter.

According to 44 USC § 3301, the definition of a Federal record is "all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor, as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them."

Linking to External Sites

If hypertext links or pointers to information created and maintained by other public and private organizations are used, the links must conform to Secret Service web development standards.

The Secret Service does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained on a linked website.

Refer to Government and Public Affairs Manual section PAF-09(02), External Links from Secret Service Public-Facing websites, for policy addressing notification requirements when a user selects a link to an external website.

Secret Service Branding on Websites

In accordance with OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications," in general, when the Secret Service uses a third-party website or application that is not part of an official government domain, the Secret Service should apply appropriate branding to distinguish the agency's activities from those of non-government actors. For example, to the extent practicable, the Secret Service seal or emblem should be added to its profile page on a social media website to indicate that it is an official agency presence.

Security/Terms of Use

A standard security statement shall be applied Secret Service-wide and shall be readily accessible from all top level, or entry point Secret Service web pages, or as deemed necessary by the CISO. Refer to the

Government and Public Affairs Manual section PAF-09(01), Posting Website Policies and Notices.

Copyright Information

Links to Secret Service websites are welcomed. Unless a copyright is indicated, information on Secret Service websites is in the public domain and may be copied and distributed without permission. Citation to the Secret Service as the source of the information is appreciated.

If a copyright is indicated on a video, photograph, graphic, or other material, permission to copy the material must be obtained from the original source.

Commercial Video and Image Website - YouTube

Although specific technologies are not generally cited in policy, since DHS has a YouTube presence on the Internet, it is specifically addressed in this directive.

Commercial sites are opportunities for supplementing how the Secret Service reaches its target audiences for recruitment, informational, or other purposes. These sites should never replace official communication channels, such as SecretService.gov.

YouTube is a public, commercial, video sharing website where users can upload, view, and share video clips. It is located at www.youtube.com. DHS will develop and maintain a YouTube.com channel for the general public featuring videos from the Department and its components (e.g., Secret Service).

DHS's YouTube presence is governed by a Content Hosting Agreement for Federal Government Agencies between the Department (DHS) and Google, Inc. (the owner of YouTube). Under this agreement, all Department channels hold a Federal "partner" status. The benefits of this status include legal protections and no advertisements on the channels, as well as more control over channel design, length of content, and feature rotations/playlists.

It is the policy of DHS to have a single Department-wide agreement with YouTube to create and maintain an official DHS YouTube.com partner channel at www.youtube.com/ushomelandsecurity. The Department will establish playlists, and sponsor and approve sub-channels as appropriate.

The DHS Assistant Secretary, Office of Public Affairs (OPA), pursuant to the provisions of Management Directive 2230, Public Affairs Management Structure, and Management Directive 2000, Organization of the Office of Public Affairs, accepts responsibility for establishing and enforcing the policies and requirements for video content on all Department channels.

The DHS Assistant Secretary, OPA, is the final authority for the approval of video content on the main Department channel and component (e.g., Secret Service) channels. The Department reserves the right to remove video content that may create a liability for the parties involved, including video content that may improperly disclose intellectual property, create a security risk, or disclose classified information.

Not all videos on DHS or Secret Service websites are required to be posted on YouTube. Videos posted on YouTube must also be posted on the Secret Service website (e.g., SecretService.gov) and follow all Department content policies, guidelines, and regulations. All video content submitted for posting on SecretService.gov will automatically be considered for posting to the Department's YouTube channel.

Content providers requesting video content on SecretService.gov who do not wish to have it posted on YouTube must provide an explanation with their file submission.

All videos must meet the general video file and content requirements of DHS as defined on DHS's Online Web Center. The Department, at the sole discretion of the DHS Assistant Secretary of Public Affairs, reserves the right to reject video submissions for failure to comply with content requirements.

To avoid the use of third party cookies, the Department must not use the YouTube "embed" feature on its own websites to distribute video.

Refer to the "DHS Public Affairs YouTube.com Guidance and Procedures" (http://www.dhs.gov/xlibrary/assets/opa_guidance_youtube_7-22-09.pdf) document for additional guidelines and requirements.

Disclaimer of Endorsement

The Secret Service does not endorse the use of or imply preference for any vendor commercial products or services.

Requests for Exceptions to this Directive

All requests for exceptions to this directive must be submitted in writing to the SAIC of Public Affairs and the Secret Service Chief Information Officer (CIO). If approved by the SAIC of Public Affairs and the CIO, the Secret Service CIO will submit a request to the DHS CIO in writing. Each request will be handled on a case-by-case basis.

Applicable Laws/Guidance

Executive Order 13556, Controlled Unclassified Information, November 4, 2010.

Pub. L. 107-347, E-Government Act of 2002, December 17, 2002.

Section 508 of the Rehabilitation Act of 1973 (as amended).

Office of Management and Budget (OMB), Memorandum M-06-02, Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model, December 16, 2005.

OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010.

OMB Circular A-130, "Management of Federal Information Resources."

DHS Management Directive (MD) 2000, Organization of the Office of Public Affairs, January 24, 2003.

DHS MD 2230, Public Affairs Management Structure, March 1, 2003.

DHS MD 4400.1, DHS Web (Internet, Intranet, and Extranet Information) and Information Systems, March 1, 2003.

DHS MD 140-01, Information Technology System Security, July 31, 2007.

DHS Sensitive Systems Policy Directive 4300A, Version 8.0, March 14, 2011.

DHS 4300A Sensitive Systems Handbook, Version 7.2.1.1, January 20, 2011.

DHS 4300A Sensitive Systems Handbook, Attachment X – Social Media, Version 8.0, May 23, 2011.

DHS Facebook Policies and Procedures, DRAFT, January 4, 2011.

DHS Privacy Impact Assessment for the Use of Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue), September 16, 2010.

DHS Privacy Impact Assessment for the Use of Unidirectional Social Media Applications Communications and Outreach, March 8, 2011.

DHS Public Affairs YouTube.com Guidance and Procedures, July 22, 2009.

DHS Online Web Center, an internal resource for public web communications. This Homeland Security Web Center, managed by the DHS Office of Public Affairs, hosts policies, procedures, and other resources to build a better Homeland Security web presence.
(http://www.dhs.gov/xother/wbcntr/editorial_0587.shtm)

General Services Administration (GSA), GSA Social Media Policy, CIO 2106.1, July 17, 2009.

GSA, GSA Social Media Handbook, CIO 2106.2, July 17, 2009.

GSA, The Social Media Navigator, GSA's Guide to Official Use of Social Media, April 2011.

National Archives and Records Administration (NARA), NARA Guidance on Managing Web Records, January 2005.

NARA, Bulletin 2011-12, Guidance on Managing Records in Web 2.0/Social Media Platforms, October 20, 2010.

NARA, Implications of Recent Web Technologies for NARA Web Guidance, undated, (http://www.archives.gov/records-mgmt/initiatives/web-tech.html).

SOCIAL MEDIA STANDARDS OF CONDUCT

Purpose

This directive establishes Secret Service policy regarding the standards of conduct for the use of social media.

Refer to the Government and Public Affairs Manual section PAF-08(03), for Guidelines for Unofficial Personal Use of Social Media on Non-Government Equipment.

Refer to the Technical Development and Mission Support Manual section IRM-10(03), for Information Technology (IT) General Rules of Behavior policy.

Refer to the Technical Development and Mission Support Manual section OPSC-01, for United States Secret Service Operational Security Program (OPSEC) policy.

Scope

This directive applies to all Secret Service employees. It also applies to contractors engaged in social media on behalf of the Secret Service as part of their duties.

Definition of Terms

Refer to the Government and Public Affairs Manual section PAF-08(07), Glossary of Social Media Terms, for the definition of terms.

Responsibilities

Office Supervisors (SAIC, RAIC, RA, or Division Chief): Each office supervisor or his/her designee is responsible for:

- Verifying that each employee assigned to their respective office has acknowledged the "Social Media Standards of Conduct" upon his/her "Enter on Duty" date and annually thereafter, by signing SSF 3218, U.S. Secret Service Employee Certification. (Refer to Human Resources and Training Manual section PER-05(01), Standards of Conduct – General);

- Ensuring that all non-Secret Service employees, to include, but not limited to, summer student assistants, interns, Foreign Service Nationals, law enforcement partners and task force members, other Government agency personnel, and contractors, assigned to their respective office have acknowledged the "Social Media Standards of Conduct" upon his/her "Enter on Duty" date and annually thereafter, by signing the SSF 4087, Non-USSS Employee Certification. The Contracting Officer's Technical Representative will retain this form in the contract files pursuant to record retention schedules for contract files. The Office Security Representative will retain the form for all other non-Secret Service employees;

- Enforcing this policy, including remedial training and other sanctions; and

- Promptly reporting misconduct in accordance with Human Resources and Training Manual section PER-05, Employee Responsibilities and Conduct; and Technical Development and Mission Support Manual section IRM-11(09), Reporting Requirements for Computer Security Incidents and Vulnerabilities. Inappropriate use is considered a security incident.

All Employees and Contractors: All employees and contractors shall:

- Comply with this and other directives prescribing the use and management of web information and associated systems while on duty and off duty; and

- Report discrepancies or policy inconsistencies reflected in web content to appropriate managers.

Policy

Standards of Conduct

Secret Service employees and contractors are responsible for knowing and following Secret Service and Department of Homeland Security (DHS) standards of conduct (refer to the Human Resources and Training Manual chapter PER-05), and Executive Branch conduct guidelines, such as the "Standards of Ethical Conduct for Employees of the Executive Branch," when using social media in an official capacity. These standards cover topics of prohibited activities such as:

- Engaging in vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups;
- Endorsement of commercial products, services, or entities;
- Endorsement of political parties, candidates, or groups;
- Lobbying members of Congress using DHS/Secret Service or any other appropriated resource; and
- Use of government resources to foster commercial interests or individual profit.

Unofficial/Personal Use of Social Media on Government Equipment is Prohibited

Although Secret Service employees are authorized limited personal use of Secret Service office equipment in accordance with Human Resources and Training Manual section PER-05(10), Use of Government Systems, this **does not apply to use of Secret Service equipment for personal use of social media**. This restriction also applies to contractors or other individuals using Secret Service equipment.

Social Media and Political Activities

The Hatch Act governs political activities by Federal employees. Under its terms, the Secret Service is a "further restricted" agency, and its employees are subject to the most stringent restrictions. Secret Service employees are, therefore, prohibited from engaging in partisan political management or campaigning. This means that Secret Service employees may not undertake any activity in concert with a partisan political candidate, party, or organization.

This prohibition has special implications in the context of social media. Employees who use social media websites may not in any way link to the sites or pages of a partisan political candidate, party, or organization. This includes "liking," "friending," being a fan of, or listing an interest in a candidate, party, or organization. In addition, employees may not repost or retweet statements by a candidate, party, or organization. Such links and reposts are considered to be distributing political material or fundraising. Employees' profiles, however, may reveal their professional titles and their political affiliations.

In spite of these restrictions, employees retain their right to express their personal opinions. Employees may also keep a blog or post a status update in which they state their political opinions. Employees should not, however, copy campaign literature from a partisan candidate, party, or organization.

The U.S. Office of Special Counsel (OSC), which enforces the Hatch Act, has issued guidance on the interaction of the Hatch Act and social media. The guidance may be found in the Hatch Act Frequently Asked Questions for Federal Employees, available on the OSC's website, www.osc.gov. Questions regarding the Hatch Act may be directed to an ethics official in the Office of Chief Counsel.

Location-Based Services (LBS)

Location-Based Services (LBS) (geolocation) technologies, also referred to as mobile location technologies or social mobile applications, typically allow users to share their real-time or historical location information online and pose privacy concerns.

With the popularity of smartphones (e.g., iPhones, BlackBerry devices) on the market, many users are now easily locatable, as are users of most wireless devices including cell phones, e-book readers, laptops, netbooks, and tablets (e.g., iPads). As Global Positioning System (GPS) and wireless networking technology capabilities have been built into an increasing number of these devices, location information has become increasingly accurate. Mobile location data identifies the exact physical whereabouts of an individual or his/her device in real or near-real time at anytime and anywhere.

Because individuals often carry their mobile devices with them, location data may be collected, often

without user interaction, and it may describe both what a person is doing and where he or she is doing it. It can reveal visits to potentially sensitive destinations.

Weak privacy protections put users at risk in two important ways. First, data collected about users may be retained long after the moment of data collection, and often long after the original location service has been provided. This data may be shared, sold, or put to unpredictable uses far in the future. The second type of risk derives from services that share consumer location with acquaintances or with the public at large. While these technologies offer new opportunities for Internet users, products built with defaults that do not protect privacy may place the uninformed user in dangerous situations.

Carrying a device with location-based services enabled could compromise an investigation or protection assignment. **Employees should not use location based social networking applications while on duty on their personal or government-issued devices, particularly at locations where presenting exact grid coordinates could adversely affect Secret Service operations.**

Unofficial Internet Posting

"Unofficial Internet posts" result when Secret Service personnel express their Secret Service-related thoughts, ideas, knowledge, experience, and opinions on any Internet site, whether Secret Service-controlled or otherwise. Unofficial Internet posts are personal expressions developed and released by an employee or contractor that have not been initiated by any part of the Secret Service organization, or reviewed within any official Secret Service approval process.

Adversaries can collect even seemingly harmless facts and use them to assemble profiles and select targets. Even with privacy controls in place, Secret Service employees and contractors should not post any content that they would not be comfortable disclosing to the public.

Any information that is work-related is sensitive and cannot be repeated outside the workplace without appropriate approvals.

Secret Service personnel who post content about the Secret Service on the Internet are responsible for ensuring that any information disclosed (including personal comments) is accurate and appropriate. Personnel should keep in mind how their posts will reflect upon themselves and the Secret Service, and also be aware that some individuals and groups use public networking forums to gain information that will help them advance their own causes or agendas at the expense of others. Secret Service personnel who engage in unofficial posting on the Internet shall observe the following:

1. Release of Secret Service e-mail addresses, telephone numbers, or facsimile numbers not already publicly released, including the content manager's or content provider's work contact information, is not authorized.

2. The posting or disclosure of internal Secret Service documents or information that Secret Service has not officially released to the public is not authorized. This policy applies no matter how the information was obtained. Examples include, but are not limited to, the following: memos, e-mails, meeting notes, articles for publications, white papers, Public Affairs guidance, and all pre-decisional materials. Additionally, information marked as sensitive or for limited use (e.g., For Official Use Only (FOUO), Controlled Unclassified Information (CUI), Law Enforcement Sensitive (LES)), and Personally Identifiable Information (PII) shall not be released in unofficial Internet posts.

3. Personnel are responsible for adhering to Secret Service policies concerning information security, physical security, and the Privacy Act, as they are in all other forms of communication. Do not

advertise real or perceived weaknesses, vulnerabilities, or loopholes in Secret Service systems or capabilities. Unauthorized disclosure of protected information may result in disciplinary action.

4. Releasing another employee's information is not authorized. Release of classified, operational, proprietary, law enforcement sensitive, or investigatory information is not authorized.

5. A photo, video, or sound recording taken of an official Secret Service activity by Secret Service personnel is considered official Secret Service media. Newsworthy media should be released officially to news organizations in conjunction with, or copied to, Public Affairs before posting unofficially.

6. Secret Service-related media taken while Secret Service personnel are in a non-working status in public areas, (e.g., photo of the President's motorcade while on a public street) is considered private imagery and is not subject to these guidelines.

7. Use of official or protected Secret Service statements or symbols (e.g., logo) must be approved by the Public Affairs Program. This requirement is needed to prevent the impression of official or implied endorsements. Refer to Government and Public Affairs Manual section PAF-05, Use of Official Insignia.

8. Release of location-based (geospatial) information related to a Secret Service mission, whether intentional or unintentional, is not authorized. For example, this includes the location of an employee and/or Secret Service asset at a particular point in time (e.g., auto-tweeting geospatial coordinates while driving, or reporting via a location-based social media tool such as Foursquare).

9. As with other forums of personal public engagement, Secret Service personnel shall avoid off-duty behavior that negatively impacts or conflicts with their ability to execute their duties for the Secret Service, such as the prohibited personal conduct described in the *Standards of Ethical Conduct for Employees of the Executive Branch.*

Refer to Government and Public Affairs Manual section PAF-08(01), Content Management on Public-Facing Websites and Social Media, for categories of information which are prohibited on public-facing websites.

Applicable Laws/Guidance

5 U.S.C. §§ 7321-7326, The Hatch Act of 1939, Political activity authorized; prohibitions.

5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.

U.S. Office of Special Counsel, Frequently Asked Questions Regarding Social Media and the Hatch Act, August 10, 2010.

Office of Management and Budget (OMB) Memorandum M-11-06, WikiLeaks – Mishandling of Classified Information, November 28, 2010.

Department of Homeland Security (DHS) Office of the General Counsel, Memorandum for Career members of the Senior Executive Service, employees of the U.S. Secret Service, U.S. Immigration and Customs Enforcement Office of Homeland Security Investigations, and Administrative Law Judges, Subject: Political Activities, September 20, 2010.

DHS MD 480.1, Ethics/Standards of Conduct.

DHS MD 140-01, Information Technology System Security, July 31, 2007.

DHS Sensitive Systems Policy Directive 4300A, Version 8.0, March 14, 2011.

DHS 4300A Sensitive Systems Handbook, Version 7.2.1.1, January 20, 2011.

DHS 4300A Sensitive Systems Handbook, Attachment X – Social Media, Version 8.0, May 23, 2011.

GUIDELINES FOR UNOFFICIAL PERSONAL USE OF SOCIAL MEDIA ON NON-GOVERNMENT EQUIPMENT

Purpose

This directive provides guidelines for the unofficial personal use of social media outside of work.

Refer to the Government and Public Affairs Manual section PAF-08(02), for the Social Media Standards of Conduct.

Refer to the Technical Development and Mission Support Manual section OPSC-01, for United States Secret Service Operational Security Program (OPSEC) policy.

Refer to the Technical Development and Mission Support Manual section IRM-10(03), for the Information Technology (IT) General Rules of Behavior policy.

Scope

This directive applies to all Secret Service employees and contractors.

Definition of Terms

Refer to the Government and Public Affairs Manual section PAF-08(07), Glossary of Social Media Terms, for the definition of terms.

Background

Employee activities potentially affect Secret Service job performance, the performance of others, or Secret Service business interests. Any information posted on the Internet incurs a level of risk, because that information is exposed indefinitely with no reliable methods for deleting or retracting the content. Additionally, because of the connected nature of the Internet, even information that is presumed to be posted in a venue with restricted access is potentially accessible to anyone.

Social networks are of particular concern because of the potential for users to disseminate personal

information about themselves. When a Federal employee joins a social media website, they may identify themselves as an employee of their department. This may happen intentionally in their profile, or unintentionally as they register with their .GOV or .MIL e-mail address. Their self-identification creates a departmental Internet footprint, which is valuable information to adversaries. As more Federal employees self-identify on social media websites, the Federal footprint on social networking will grow, creating an environment to help adversaries target specific individuals to launch various social engineering and spear phishing attacks.

For example, an adversary may learn personal information about an individual and build a trust relationship by expressing interest in similar topics. Once the victim trusts the adversary, the adversary can collect more information about the user, or use their relationship to expand their influence. The adversary can expand their trust relationship to other users and friends, further gathering information and penetrating the trust of departmental personnel.

Additionally, high-profile Federal employees create an even larger footprint, as they have greater name recognition, collect more friends, and often want to engage with the public. A high-profile Federal employee with greater name recognition is a prime target for a social engineer to exploit the trust relationships established within that social network. Through a compromised social media account, the adversary may pose as a friend to elicit information, action, or support.

Unless strict privacy controls are applied to online profiles, the information posted is viewable by a wide range of strangers. Adversaries can collect that information – even seemingly harmless facts – and use it to assemble profiles and select targets. Whereas normally adversaries would have to engage in detailed information gathering to collect sensitive information, social networks provide a single source from which to gather this information with relative ease. Even with privacy controls in place, Secret Service employees and contractors should not post any content that they would not be comfortable disclosing to the public.

Guidelines

The following are best practices for the personal use of social media by Secret Service employees and contractors outside of work. These best practices are based on guidelines established by other Federal and commercial organizations.

Online activities often blur the line between an individual's personal and professional lives. Real-world social and business rules have counterparts in digital environments. Activities of Secret Service employees or contractors, within or outside the workplace may affect their Secret Service job performance, the performance of others, or Secret Service business interests so they are a proper focus for best practice guidance, and in some circumstances, may give rise to grounds for disciplinary and/or clearance-related actions.

The following guidelines are intended to assist Secret Service employees and contractors in protecting their personal information and reputation while interacting online in an unofficial/personal capacity.

1. **PERSONAL USE OF SOCIAL MEDIA** should be done on personal time using a personally-owned computer and e-mail account. Personnel shall not be logged into external social networking sites while at work.

2. **NO CLASSIFED INFORMATION**. Do not post classified or sensitive information. This can lead to significant adverse action and penalties.

3. **DO NOT COMMUNICATE SECRET SERVICE POLICIES**. Do not answer questions or make statements about or on behalf of the Secret Service on a social networking site without explicit authorization from the Public Affairs Program or the Chief Counsel's Office.

4. **IF IN DOUBT, SEEK GUIDANCE.** Seek guidance from the Public Affairs Program and/or the Chief Counsel's Office prior to sharing publicly any personal opinions or statements based on your role within the Secret Service. Those with leadership responsibilities, by virtue of their position, especially must understand that personal thoughts they publish, even in clearly personal venues, inadvertently may be interpreted as expressions of official Secret Service positions. They should assume that their co-workers, employees, and those outside of Secret Service will read what they have written.

5. **LIMIT THE AMOUNT OF PERSONAL INFORMATION YOU WILLINGLY POST TO SOCIAL NETWORKS**. Avoid posting information such as your home address, personal phone numbers, or details about your schedule or routine. Do not openly associate yourself with the Secret Service and do not promote your personal or professional responsibilities in your profile(s) or postings. Do not provide details regarding your work associates/colleagues, official position, duties, or training. This type of information gives cyber criminals the baseline they need for more targeted activities. Assume that anything you might post to a social network can be seen by anyone and act accordingly. Also, be wary of the type of information — including photographs — that you post about your friends and family, since that information can put them at risk.

6. **HAVE NO EXPECTATIONS OF PRIVACY**. You should assume your posts are in the public domain, even when using privacy controls, as public social media privacy controls have been known to fail. Remember that social networking sites are generally public and permanent, even if you delete the information you posted. You should understand the security and privacy features available for the social networking sites you use, and exercise discretion and common sense. Do not post anything that you would not want the public to see. Most social networks offer settings to keep profiles private and restrict access to your photographs or other personally identifiable details; however, opting for privacy does not guarantee others will not see your content. Content can be forwarded or hacked. If you allow your messages to travel between different social networks, privacy becomes more complicated. Information you trust to your friends might end up somewhere else. Hackers can force access, and friends can forward your content.

7. **USE THE PRIVACY/SECURITY SETTINGS.** When accessing social networking sites, you can limit disclosure by using the Privacy settings that are available. The default settings for some sites may allow anyone to see your profile. You can customize your settings to restrict access to only certain people. Also be aware of any changes to the site's privacy/security options. For example, in 2009 Facebook made major changes to user privacy settings. Some of the new settings replaced previous settings and reset them to be "viewable by everyone." Users should monitor the privacy policies for social networking sites as they change often and without warning. Remember though, there is a risk that even private information can be exposed, so do not post anything that you would not want the public to see.

8. **BE AWARE OF PRIVACY AND SECURITY ISSUES WHEN USING LOCATION-BASED SERVICES (LBS).** Location-based services offer many conveniences such as keeping track of family and friends, getting directions, finding restaurants, and assisting in law enforcement. However, information about your location may be accessible to unintended recipients. Use of LBS introduces significant privacy and personal security risks with their use. The most common example is using a location check-in service (i.e., Foursquare). If you check in from your couch, the precise Global Positioning System (GPS) coordinates of your couch, in your home, are published. If you then check in from your office, it can be established that you are no longer at your home and your home would be an excellent target. This mere fact can compromise your own personal security.

   Employees should also be aware that this information may leak unintentionally. For example, smart

phones can attach GPS coordinates to pictures you take. Posts made to social media sites such as Facebook or Twitter may also contain this detailed geo-location data that could compromise your personal security and possibly your workplace security.

Be sure to examine your phone's privacy, security, and location settings to ensure that GPS coordinates are not automatically associated with services. Be sure never to check in from sensitive locations and avoid establishing patterns where possible.

9. **PROTECT PRIVACY**. You should not share personal or contact information about your family, friends, co-workers, clients, or businesses without that individual's explicit consent. You also should not post or tag pictures of family, friends, co-workers, clients, or business without their consent. At all times, respect the privacy of others. You should always protect sensitive information such as personally identifiable information (PII).

10. **RESPECT COPYRIGHT, FAIR USE, AND FINANCIAL DISCLOSURE LAWS**. Do not post any information or other material protected by copyright without the permission of the copyright owner.

11. **DO NOT BREACH TRADEMARKS**. Do not use any words, logos, or other marks that would infringe upon the trademark, service mark, certification mark, or other intellectual property rights of the owners of such marks without the permission of such owners.

12. **USE DISCLAIMERS**. Be aware of your Secret Service association in online social networks. If your profile reveals your employment relationship with the Secret Service, you should include a disclaimer stating that your activity and posts represent your personal opinions and do not represent those of the Secret Service. An example of an appropriate disclaimer is "The postings on this site are my own and do not represent Secret Service positions, strategies, or opinions." Never use or reference your formal position when writing in a non-official capacity. Consult the Public Affairs Program and/or the Chief Counsel's Office when in doubt. Those with leadership responsibilities, by virtue of their position, must consider whether personal thoughts they publish, even in clearly personal venues, may be misunderstood as expressing Secret Service positions.

13. **BE PROFESSIONAL**. If you identify yourself as a Secret Service employee or have a public-facing position for which your Secret Service association is known to the general public, ensure your profile and related content is consistent with how you wish to present yourself as a Secret Service professional, even if it is of a personal and unofficial nature. Ensure all your posts and interactions are consistent with the public trust associated with your position, and conform to existing standards such as the *Standards of Ethical Conduct for Employees of the Executive Branch*.

14. **AVOID THE OFFENSIVE**. Do not post any defamatory, libelous, vulgar, obscene, abusive, profane, threatening, racially and ethnically hateful, or otherwise offensive or illegal information or material.

15. **BE THE FIRST TO RESPOND TO YOUR OWN MISTAKES.** If you make an error, be up front about your mistake and correct it quickly. In a blog, if you choose to modify an earlier post, make it clear that you have done so.

16. **BE YOURSELF**. Do not forge or otherwise manipulate identities in your posts in an attempt to disguise, impersonate, or otherwise misrepresent your identity or affiliation with any other person or entity.

17. **BE JUDICIOUS ABOUT INSTALLING APPLICATIONS FROM SOCIAL MEDIA SITES.** Often, these applications are given full access to your personal information not necessary for operation, but supplied by granting total access to your account to the application. "Quizzes" are also problematic. For example, Facebook users taking quizzes can reveal far more personal information to applications than they realize. This is mostly due to the fact that Facebook's default privacy settings allow access to all your profile information whether or not your profile is set to "private." Even if you

do not take quizzes yourself, your profile information is revealed when one of your friends takes a quiz. Almost everything on your profile, even if you use privacy settings to limit access, is available to the quiz.

18. **BE SKEPTICAL ABOUT ALL LINKS**. Vigilance is the best defense against phishing. Phishing scams can arrive in e-mails that look as though they come from real companies or trusted individuals. For example, you may receive an e-mail message announcing that your bank account will be closed unless you confirm your personal identification number, or one claiming you need to provide your credit card information to confirm an order, or requesting verification of your Social Security number for billing purposes.

    Legitimate companies do not ask for your account or personal information via e-mail. To find out whether the message is legitimate, contact the company directly by telephone or letter using data from a trusted source, such as your account statements or the back of your credit/debit card. Instead of simply clicking on an embedded link, manually type the Uniform Resource Locator (URL) into the navigation bar of your web browser to avoid clickjacking.

    Phishing attempts can also come in tweets (see Twitter), Facebook wall postings, videos, or pictures. For example, a friend sending a link to a funny video might have had his/her account compromised. Get into the habit of not clicking on hyperlinks, especially those for videos or news-related events. In many cases, these are linked to phishing and social engineering attacks.

19. **USE STRONG PASSWORDS**. Protect your account with passwords that cannot be easily guessed. Passwords should include a combination of upper and lowercase letters, numbers, and special characters. Do not use the password you use to access non-Secret Service information technology (IT) systems or services, such as your personal Internet or e-mail account, to access Secret Service IT systems and services. Refer to Technical Development and Mission Support Manual section IRM-12(02), Password Change Policy, for guidelines for selecting and protecting your password.

Social Media and Political Activities

The Hatch Act governs political activities by Federal employees. Under its terms, the Secret Service is a "further restricted" agency, and its employees are subject to the most stringent restrictions. Secret Service employees are, therefore, prohibited from engaging in partisan political management or campaigning. This means that Secret Service employees may not undertake any activity in concert with a partisan political candidate, party, or organization.

This prohibition has special implications in the context of social media. Employees who use social media websites may not in any way link to the sites or pages of a partisan political candidate, party, or organization. This includes "liking," "friending," being a fan of, or listing an interest in a candidate, party, or organization. In addition, employees may not repost or retweet statements by a candidate, party, or organization. Such links and reposts are considered to be distributing political material or fundraising. Employees' profiles, however, may reveal their professional titles and their political affiliations.

In spite of these restrictions, employees retain their right to express their personal opinions. Employees may also keep a blog or post a status update in which they state their political opinions. Employees should not, however, copy campaign literature from a partisan candidate, party, or organization.

The U.S. Office of Special Counsel (OSC), which enforces the Hatch Act, has issued guidance on the interaction of the Hatch Act and social media. The guidance may be found in the Hatch Act Frequently Asked Questions for Federal Employees, available on the OSC's website, www.osc.gov. Questions regarding the Hatch Act may be directed to an ethics official in the Office of Chief Counsel.

SOCIAL MEDIA AND PRIVACY ISSUES

Purpose

This directive establishes Secret Service policy regarding social media and personally identifiable information (PII).

Refer to Government and Public Affairs Manual section PAF-09(01), Posting Website Policies and Notices, for required privacy statement language on public-facing Secret Service websites.

Scope

This directive applies to all Secret Service employees. It also applies to contractors engaged in social media on behalf of the Secret Service as part of their duties.

The scope of this directive is limited to the use and management of Secret Service web information and associated systems where the intent is to make information available to the public, or to a general audience within the Department of Homeland Security (DHS or Department).

This directive does not apply to internal Secret Service activities (such as on Intranets, applications, or interactions that do not involve the public), or to activities that are part of authorized law enforcement, national security, or intelligence activities.

Definition of Terms

Refer to the Government and Public Affairs Manual section PAF-08(07), Glossary of Social Media Terms, for the definition of terms.

Background

Privacy laws require the protection of PII and require Secret Service to engage the public in a manner that protects privacy in compliance with those privacy laws.

Federal public websites are required to conduct privacy impact assessments (PIA) if they collect PII, post a "Privacy Act Statement" that describes the agency's legal authority for collecting personal data and how the data will be used, and post privacy policies on each website.

Office of Management and Budget (OMB) policy mandates that Federal websites are prohibited from using persistent cookies and other web tracking methods unless their use has been approved by an agency head or designated agency sub-head, for a compelling need. When approved in this fashion, agencies must post clear notice of the nature of the information collected in the cookies, the purpose and use of the information, whether or not and to whom the information will be disclosed, and the privacy safeguards applied to the information collected, as described in OMB Memorandum M-03-22.

The Secret Service is bound to protect PII on internal websites and pages on external social media websites. The Privacy Act of 1974 (as amended) may also apply to the activities undertaken on social media platforms, and individuals should consult with the Secret Service Disclosure Officer and the Chief Counsel to ensure they are in compliance with all privacy protection requirements.

The Secret Service will not share or sell any personal information obtained from users with any other organization or government agency except as required by law.

Responsibilities

Chief Counsel: The Office of the Chief Counsel provides advice and assistance on all legal matters arising out of, or incident to, the use of social media.

Special Agent in Charge (SAIC), Public Affairs Program, GPA: The SAIC, Public Affairs Program, serves as the Secret Service's central point of contact for posting content to social media and public-facing websites. The SAIC of Public Affairs is responsible for ensuring that website initiatives adhere to policies, laws, regulations, and guidance regarding privacy.

Disclosure Officer: The Disclosure Officer is the privacy point of contact for the Secret Service. The Disclosure Officer is responsible for privacy compliance across the Secret Service, including assuring that technologies used by the Secret Service sustain and do not erode privacy protections relating to the use of personal and Secret Service information. The Disclosure Officer is responsible for ensuring that Secret Service's use of social media sustains and does not erode privacy protections concerning the use, collection, and disclosure of PII.

Employees and Contractors: Secret Service employees and contractors must comply with Federal privacy laws, Office of Management and Budget (OMB) guidance, and DHS/Secret Service privacy policies when using social media in an official capacity.

Policy

1. When the Secret Service uses social networking websites and applications, it shall not:

   - Actively seek PII, and may only use the minimum amount of PII it receives, which is necessary to accomplish a purpose required by statute, Executive Order, or regulation. All other PII received will be managed in accordance with the requirements and analytical understanding outlined in the Department of Homeland Security (DHS) Privacy Impact Assessment (PIA) for the Use of Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue);

   - Search social networking websites or applications for or by PII; and

- "Friend" public users proactively. The Secret Service may, however, "friend" other U.S. Federal, State, local, and tribal government agencies. Requests to "friend" other non-government entities, such as media outlets or mission-related non-governmental organizations, may be made by submitting a waiver request to the Secret Service Disclosure Officer who will coordinate with the DHS Privacy Office.

2. DHS has set forth specific requirements on how the Department and its components (e.g., Secret Service) may engage in social networking including the use of applications in a privacy sensitive way. Refer to DHS's Privacy Impact Assessment (PIA) for the Use of Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue), which can be found at http://www.dhs.gov/privacy.

   The PIA addresses the PII the Department and its components may have access to due to its use of social networking applications, how it will use the information, what information is retained and shared, and how individuals can gain access to and correct their information. DHS and the Secret Service do not solicit, collect, or disseminate PII from individuals who interact with the DHS/Secret Service via social media sites.

   If PII is posted on a social networking website or application, or sent to the Secret Service in connection with the transaction of public business, it may become a Federal record and, if so, the Secret Service is required to maintain a copy per its records retention policies. If content does contain privacy information, the content may be removed from the application or site, and transferred to a different media source for records retention.

   If PII is posted on a social media site that is not related to the transaction of public business, the DHS/Secret Service will attempt to delete it. If that is not possible, the DHS/Secret Service will disregard the PII.

   Refer to the Professional Responsibility Manual chapter MNO-6, for Records Management policy.

3. If the Secret Service has an operational need to use social media outside the scope of the requirements outlined in the existing DHS PIA, a separate PIA must be completed and approved by the appropriate privacy official. That PIA should address the specific privacy concerns that are unique to the Secret Service. Otherwise, the Secret Service can apply the existing PIAs to its social media applications by submitting a Privacy Threshold Assessment (PTA) to the Disclosure Officer detailing how the application has met the outlined requirements.

Use of Third-Party Websites or Applications – Privacy Requirements

When the Secret Service uses third-party websites and applications to engage openly with the public, it must comply with the requirements of OMB memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications," dated June 25, 2010, to ensure that privacy is fully protected.

1. **Third-Party Privacy Policies.** Before using any third-party website or application to engage with the public, the third party's privacy policy shall be examined to evaluate the risks and determine whether the website or application is appropriate for the Secret Service's use. In addition, the Public Affairs Program shall monitor any changes to the third party's privacy policy and periodically reassess the risks.

2. **External Links.** If the Secret Service posts a link that leads to a third-party website or any other location that is not part of an official Government domain, the Secret Service shall provide an alert to the visitor, such as a statement adjacent to the link or a "pop-up," explaining that visitors are being

directed to a non-Government website that may have different privacy policies from those of the Secret Service's official website.

3. **Embedded Applications.** If the Secret Service incorporates or embeds a third-party application on its website or any other official Government domain, the Secret Service shall take the necessary steps to disclose the third party's involvement and describe the Secret Service's activities in its privacy policy, as specified in OMB memorandum M-10-23.

4. **Agency Branding.** In general, when the Secret Service uses a third-party website or application that is not part of an official Government domain, the Secret Service should apply appropriate branding to distinguish the Agency's activities from those of non-government actors. For example, to the extent practicable, the Secret Service seal or emblem should be added to its profile page on a social media website to indicate that it is an official agency presence.

5. **Information Collection.** If information is collected through the Secret Service's use of a third-party website or application, the Secret Service should collect only the information "necessary for the proper performance of agency functions and which has practical utility" as described in OMB Circular A-130. If PII is collected, the Secret Service shall collect only the minimum necessary to accomplish a purpose required by statute, regulation, or Executive Order.

   If the Secret Service asks the public to respond to a series of specific questions or a series of specific prompts that gather information (e.g., for purposes of aggregation or survey) about whether, for example, a particular program is or is not effective, the collection of information is subject to the Paperwork Reduction Act (PRA). However, the PRA does not apply to posts that allow members of the public to provide general or unstructured feedback about a program (such as a standard *Federal Register* notice, a request for comments on a report or proposed initiative, or a request for ideas, comments, suggestions, or anything else that might improve the program).

Privacy Policy and Notice for Use of Third-Party Websites and Applications

When the Secret Service uses third-party websites and applications to engage openly with the public, it must comply with the requirements of OMB memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications," dated June 25, 2010, to ensure that privacy is fully protected.

The Secret Service's general privacy policy shall describe the Secret Service's use of third-party websites and applications, including:

- The specific purpose of the use of the third-party websites or applications;
- How the Secret Service will use PII that becomes available through the use of the third-party websites or applications;
- Who at the Secret Service will have access to PII;
- With whom PII will be shared outside the Secret Service;
- Whether and how the Secret Service will maintain PII, and for how long;
- How the Secret Service will secure PII that it uses or maintains; and

- What other privacy risks exist and how the Secret Service will mitigate those risks.

To the extent feasible, the Secret Service should post a Privacy Notice, described below, on the third-party website or application itself. The Privacy Notice should:

- Explain that the website or application is not a Government website or application, that it is controlled or operated by a third party, and that the Secret Service's privacy policy does not apply to the third party;
- Indicate whether and how the Secret Service will maintain, use, or share PII that becomes available through the use of the third-party website or application;
- Explain that by using the website or application to communicate with the Secret Service, individuals may be providing non-government third parties access to PII;
- Direct individuals to the Secret Service's official website; and
- Direct individuals to the Secret Service's privacy policy as described above.

All practical steps should be taken to ensure that the Privacy Notice is conspicuous, salient, clearly labeled, written in plain language, and prominently displayed at all locations where the public might make PII available to the agency.

Refer to PAF-09(01), Posting Website Policies and Notices, for policy addressing the requirement to post privacy policies and privacy notices.

Applicable Laws/Guidance

6 U.S.C. § 142, "Privacy Officer."

5 U.S.C. § 552a, the Privacy Act of 1974.

Office of Management and Budget (OMB) Memorandum M-11-02, Sharing Data While Protecting Privacy, November 3, 2010.

OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010.

OMB Memorandum (no number assigned), Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act, April 7, 2010.

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.

DHS Privacy Impact Assessment for the Use of Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue), September 16, 2010.

SOCIAL MEDIA RISK MITIGATION STRATEGIES

Purpose

This directive establishes Secret Service policy regarding risk mitigation strategies related to the use of social media.

Social media tools are valuable in areas such as recruitment, public affairs, and information sharing with Secret Service partners. However, as with any Internet-based capabilities, there are implementation challenges and operational risks that must be understood and mitigated.

Scope

This directive applies to all Secret Service employees. It also applies to contractors engaged in social media on behalf of the Secret Service as part of their duties.

The scope of this directive is limited to the use and management of Secret Service web information and associated systems where the intent is to make information available to the public, or to a general audience within the Department of Homeland Security (DHS or Department) outside of the Secret Service.

This directive does not apply to internal Secret Service activities (such as on Intranets, applications, or interactions that do not involve the public) or to activities that are part of authorized law enforcement, national security, or intelligence activities.

This directive addresses the non-technical security controls including policy controls, acquisition controls, and specialized training.

Refer to the Technical Development and Mission Support Manual, IRM chapter, for technical host and network controls such as standardizing the desktop image and securing the Internet connection through a Trusted Internet Connection (TIC).

Definition of Terms

Refer to the Government and Public Affairs Manual section PAF-08(07), Glossary of Social Media Terms, for the definition of terms.

Background

The decision to embrace social media technology is a risk-based decision, not a technology-based decision. The decision must be made using strong business justifications that identify mission requirements and drive toward an expected outcome through social media use. Consideration must be given to its mission space, threats, technical capabilities, and potential benefits.

Whether or not to engage in social media use is a business decision, and comes from a risk management process made by the mission owners with input from all stakeholders, including the Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Counsel, Public Affairs Program, privacy officials and the mission owner. This decision can only be made with a full understanding of the threats, risks, and mission needs.

Federal Government information systems are targeted by persistent, pervasive, and aggressive threats. In order to defend against rapidly evolving social media threats, a multi-layered approach in a risk management program is needed which addresses risks to the individual, risks to the Secret Service, and risks to the Federal infrastructure.

This directive addresses the non-technical security controls including policy controls, acquisition controls, and specialized training. Refer to the Technical Development and Mission Support Manual, IRM chapter, for technical host and network controls such as standardizing the desktop image to securing the Internet connection through a Trusted Internet Connection (TIC).

Responsibilities

Assistant Director of Government and Public Affairs (GPA): The Assistant Director of Government and Public Affairs or designee shall be responsible for the implementation of this directive.

Special Agent in Charge (SAIC), Public Affairs Program, GPA: The SAIC, Public Affairs Program, serves as the Secret Service's central point of contact for the Secret Service's use of social media.

Chief Records Officer (CRO): Management and Organization Division's (MNO) Chief Records Officer is responsible for coordinating with and assisting the Public Affairs Program to ensure social media records are properly identified, managed, and handled in accordance with National Archives and Records Administration (NARA)-approved schedules, including those specifically developed for social media content.

Office of Human Resources and Training (HRT): The James J. Rowley Training Center, Office of HRT, in tandem with DHS requirements, delivers annual mandatory online information security awareness training, including social media awareness, to all employees.

Chief Information Officer (CIO): The CIO Program is responsible for performing risk assessments for any proposed use of social media/networking. In coordination with the Chief Enterprise Architect, the CIO incorporates the current state of risk and decision science into the Enterprise Data Architecture.

Operations Security Program (OPSEC): OPSEC is responsible for providing security awareness and information-handling training to all Secret Service employees for purposes of mitigating the inadvertent compromise of sensitive and/or classified Secret Service information and/or operations.

Policy

Risk and Mitigation Related to User Behavior

Risk: Social media presents a new set of tools for interactive dialog. However, users may make themselves vulnerable by trusting circles of friends and colleagues and disclosing personal facts more readily. Additionally, phishing, social engineering, and malicious software may be used to exploit a friend's trust.

Mitigation: The safe use of social media is fundamentally a behavioral issue, not a technology issue. Policy addressing behavior associated with the risk of using social media tools, both personally and professionally, when accessing data or distributing Government information can be found in the following policies:

- Government and Public Affairs Manual section PAF-08(02), Social Media Standards of Conduct;
- Government and Public Affairs Manual section PAF-08(03), Guidelines for Unofficial Personal Use of Social Media Outside of Work; and
- Technical Development and Mission Support Manual section IRM-10(03), for the General IT (Information Technology) Rules of Behavior policy.

Risk and Mitigation Related to Social Media Hosting

Risk: Many social media and emerging technologies are outsourced and exist in a cloud computing environment. Additional security controls must be considered when using an externally hosted information system, including additional monitoring and configuration controls specific to Federal information systems.

Mitigation: The CIO shall require enhanced security and privacy controls for contracted social media services. Refer to the CIO Council's *Guidelines for Secure Use of Social Media by Federal Departments and Agencies* for specific recommendations and guidance.

Risk and Mitigation Related to Training

Risk: Users are almost always the weakest link in an information system, and may inadvertently divulge sensitive information through a social network. Few effective technical security controls exist that can defend against clever social engineering attacks. Often the best solution is to provide periodic awareness and training of policy, guidance, and best practices.

Mitigation: Due to additional attack vectors and security concerns from using social media, augmented training requirements must be considered for Federal employees and contractors. The proper use of social media in the Federal Government shall be part of the annual security awareness training.

The James J. Rowley Training Center, in partnership with other directorates, shall ensure all employees

complete the mandatory online annual awareness courses such as, but not limited to, information technology security awareness training, Sensitive Compartmented Information (SCI) refresher training, and Suspicious Activity Reporting (SAR) training. The courses shall cover, but are not limited to, the following issues:

- Provide specialized training to educate employees about what information to share, with whom they can share it, and what not to share.
- Provide guidance and training based on Public Affairs' social media policies and guidelines, and IRM-10(03) Information Technology (IT) General Rules of Behavior.
- Provide guidance to employees to be mindful of blurring their personal and professional life. Do not establish relationships with working groups or affiliations that may reveal sensitive information about their job responsibilities.
- Provide Operations Security (OPSEC) awareness and training to educate users about the risks of information disclosure when using social media, and make them aware of various attack mechanisms.
- Provide employees with additional guidance concerning if and how they should identify themselves on social media websites, depending on their official role.
- Provide specialized awareness and training on Privacy Act requirements and restrictions. Educate users about social networking privacy controls to help them take control of their own privacy, both in their personal profile and any profile they use for work-related activities.
- Educate users about specific social media threats before they are granted access to social media websites. Users may be desensitized to openly granting unnecessary access to their private information. For example, users may click "OK" without reading the full message and understanding the permissions they are granting.

Risk and Mitigation Related to Characterization of the Information

Risk: There is a risk that Secret Service users, acting in their official capacity, may "friend" public users without the public users being aware of it. This could lead public users to believe the Secret Service is inappropriately engaging with the public.

Mitigation: To mitigate this risk, the Department of Homeland Security (Department or DHS) has established requirements in the DHS Privacy Impact Assessment (PIA) for the Use of Social Networking Interactions and Applications that no Department user (to include Secret Service), acting in his/her official capacity, may actively "friend" a public user.

Secret Service users, acting in their official capacity, may accept "friend" requests from public user accounts for external relations (communications/outreach/public dialogue), to provide information about or from the Secret Service, and to provide customer service. The Secret Service uses these non-governmental websites to make information and services widely available, while promoting transparency and accountability. The Secret Service shall not "friend" public users proactively. The Secret Service may, however, "friend" other U.S. Federal, state, local, and tribal government agencies.

Personnel wishing to "friend" other non-government entities, such as media outlets or mission-related non-governmental organizations (NGOs), shall submit a waiver from this requirement to the Public Affairs Program. Users may only accept requests from the public to be "friended."

Risk: Given the nature of social networking websites and applications, personally identifiable information (PII) may transit and be displayed by the system during the sign-up/log-on transaction and subsequent interactions. All interactions may expose Secret Service employees maintaining the site to PII and that information may be inappropriately incorporated into Secret Service files. In instances where bi-directional communication with the Secret Service (chat/comment) is initiated by a public user, those remarks may be collected by the Secret Service. If PII is posted on a social networking website or application, or sent to the Secret Service in connection with the transaction of public business, it may become a Federal record and, if so, the Secret Service is required to maintain a copy per its records retention policies. Another risk is that public users may post inappropriate content on Secret Service-sponsored pages.

Mitigation: To mitigate this risk, the Secret Service recommends public users not post PII on Secret Service social networking websites or applications, or share it with the Secret Service. Additionally, if inappropriate comments (vulgar/profanity) are posted on Secret Service-sponsored pages, the Secret Service may first attempt to remove it from the page, but it may remain a Federal record in Secret Service files in accordance with record retention policies.

Risk: Public users may post specific information, including PII, to the Secret Service asking about why a particular benefit has or has not been provided.

Mitigation: The Secret Service will post a notice on all Secret Service social networking websites and applications stating that if PII is posted on a social networking website or application, or sent to the Secret Service in connection with the transaction of public business, it may become a Federal record and, if so, the Secret Service is required to maintain a copy per its records retention policies. The use of a social networking website or application to conduct communications and transactions on behalf of the Secret Service does not preclude the Secret Service's responsibility for potentially managing it as a Federal record.

Risk and Mitigation Related to the Uses of Information

Risk: PII posted on Secret Service social networking websites or applications, or sent to the Secret Service in connection with the transaction of public business may become a Federal record and, if so, the Secret Service is required to maintain a copy per its records retention policies.

Mitigation: To mitigate the risk, users should not post or send PII to the Secret Service. Users should limit the use of PII to that which is absolutely necessary.

Risk and Mitigation Related to Retention

Risk: Retaining information for longer than is relevant and necessary can introduce privacy risks such as unauthorized use and disclosure.

Mitigation: To mitigate this risk, the Secret Service will only maintain information on the social networking website or application posted by or to the Secret Service in connection with the transaction of public business as long as required by law. The DHS Enterprise Records Disposition Schedule titled "U.S. Department of Homeland Security Department-wide Schedule for Social Media Websites" serves as the primary authority regarding records retention and disposition for records of this type.

Risk and Mitigation Related to Information Sharing

Risk: Sharing too much information, particularly bi-directional communication records, is a risk inherent in this process.

Mitigation: Secret Service employees share only as much information as necessary in the performance of official Secret Service duties with those who have a need-to-know. Secret Service employees and contractors shall be trained on the appropriate use and sharing of social networking information. Secret Service employees and contractors are provided annual privacy training. Content approvers and content posters are provided additional training by Public Affairs Program officials.

Applicable Laws/Guidance

DHS Privacy Impact Assessment for the Use of Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue), September 16, 2010.

DHS Directive 007-03, Integrated Risk Management, March 28, 2011.

CIO Council, Guidelines for Secure Use of Social Media by Federal Departments and Agencies, Version 1.0, September 2009.

SOCIAL MEDIA AUTHORITIES AND GUIDANCE

This directive defines the legal authorities and guidance regarding the use of social media.

The President's Transparency and Open Government Memorandum (January 21, 2009), and the Office of Management and Budget (OMB) Director's Open Government Directive Memorandum (December 8, 2009) direct Federal departments and agencies to harness new technologies to engage the public, and serve as one of the primary authorities motivating the Department of Homeland Security's (DHS) efforts to utilize social networking websites and applications.

As a result of this new technological relationship between DHS/Secret Service and the public, it is imperative that the Secret Service engage the public in a manner that complies with Federal accessibility, privacy, information security, and records laws. The Office of the Chief Counsel, Equal Employment Opportunity (EEO) Program, Freedom of Information Act and Privacy Act Program, Public Affairs Program, Chief Information Officer Program/Chief Information Security Officer, and Management and Organization Division's Record Programs Management Branch will collaborate to ensure that all Secret Service activities related to social media are evaluated to ensure compliance issues are considered and coordinated before implementation.

Authorities supporting the Secret Service's use of social networking websites and applications include:

Executive Order 13556, Controlled Unclassified Information, November 4, 2010.

The President's Memorandum on Transparency and Open Government, January 21, 2009.

6 U.S.C. § 112, "Secretary; functions."

6 U.S.C. § 142, "Privacy Officer."

5 U.S.C. § 301, the Federal Records Act.

5 U.S.C. § 552a, the Privacy Act of 1974.

5, U.S.C. §§ 7321-7326, The Hatch Act of 1939, Political activity authorized; prohibitions.

18 U.S.C. § 1913, "Lobbying with appropriated moneys."

29 U.S.C. § 794d, Section 508 of the Rehabilitation Act of 1973 (as amended).

Section 222 of the Homeland Security Act of 2002.

Pub. L. 107-347, E-Government Act of 2002, December 17, 2002.

Children's Online Privacy Protection Act (COPPA) of 1998.

5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.

36 C.F.R. Part 1222, Creation and Maintenance of Federal Records, November 2, 2009.

Department of Homeland Security (DHS) Office of the General Counsel, Memorandum for Career members of the Senior Executive Service, employees of the U.S. Secret Service, U.S. Immigration and Customs Enforcement Office of Homeland Security Investigations, and Administrative Law Judges, Subject: Political Activities, September 20, 2010.

U.S. Office of Special Counsel, Frequently Asked Questions Regarding Social Media and the Hatch Act, August 10, 2010.

Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources".

OMB Memorandum M-11-06, WikiLeaks – Mishandling of Classified Information, November 28, 2010.

OMB Memorandum M-11-02, Sharing Data While Protecting Privacy, November 3, 2010.

OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010.

OMB Memorandum (no number assigned), Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act, April 7, 2010.

OMB Memorandum M-10-06, Open Government Directive, December 8, 2009.

OMB, Memorandum M-06-02, Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model, December 16, 2005.

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.

OMB Memorandum for the Heads of Executive Departments and Agencies, and Independent Regulatory Agencies; Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act; April 7, 2010.

Secretary of Homeland Security, Efficiency Review, Section III, Office of Public Affairs Cross-Component Coordination Task Force Directive.

DHS Management Directive (MD) 2000, Organization of the Office of Public Affairs, January 24, 2003.

DHS MD 2230, Public Affairs Management Structure, March 1, 2003.

DHS MD 4400.1, DHS Web (Internet, Intranet, and Extranet Information) and Information Systems, March 1, 2003.

DHS MD 480.1, Ethics/Standards of Conduct.

DHS MD 140-01, Information Technology System Security, July 31, 2007.

DHS Sensitive Systems Policy Directive 4300A, Version 8.0, March 14, 2011.

DHS 4300A Sensitive Systems Handbook, Version 7.2.1.1, January 20, 2011.

DHS 4300A Sensitive Systems Handbook, Attachment X – Social Media, Version 8.0, May 23, 2011.

DHS Instruction 141-01-001, Records Procedural Instruction Condensed, DRAFT, November 2010.

DHS Privacy Impact Assessment for the Use of Social Networking Interactions and Applications (Communications/Outreach/Public Dialogue), September 16, 2010.

DHS Privacy Office, Government 2.0: Privacy and Best Practices Report on the DHS Privacy Office Public Workshop, June 22 and 23, 2009, November 2009.

DHS Online Web Center, an internal resource for public Web communications. This Homeland Security Web Center, managed by the DHS Office of Public Affairs, hosts policies, procedures, and other resources to build a better Homeland Security Web presence. (http://www.dhs.gov/xother/wbcntr/editorial_0587.shtm)

DHS Public Affairs YouTube.com Guidance and Procedures, July 22, 2009.

DHS Directive 007-03, Integrated Risk Management, March 28, 2011.

CIO Council, Guidelines for Secure Use of Social Media by Federal Departments and Agencies, Version 1.0, September 2009.

General Services Administration (GSA), GSA Social Media Policy, CIO 2106.1, July 17, 2009.

GSA, GSA Social Media Handbook, CIO 2106.2, July 17, 2009.

GSA, The Social Media Navigator, GSA's Guide to Official Use of Social Media, April 2011.

National Archives and Records Administration (NARA), NARA Guidance on Managing Web Records, January 2005.

NARA, Bulletin 2011-12, Guidance on Managing Records in Web 2.0/Social Media Platforms, October 20, 2010.

NARA, Implications of Recent Web Technologies for NARA Web Guidance, undated, (http://www.archives.gov/records-mgmt/initiatives/web-tech.html).

GLOSSARY OF SOCIAL MEDIA TERMS

Auto-tweeting: A twitter account is set up to automatically notify (tweet) followers whenever the tweeter posts a new blog entry.

Blog: This term is an abbreviation for "weblog." A blog is a web-based forum where individual content providers contribute regular entries or "posts" in the form of commentary, descriptions of events, or other materials on the website. Visitors to the blog may add their own comments to the posts. Blogs may be "moderated," where the blog owner oversees the removal of any objectionable material, or they may be "unmoderated," in which case there is no external control on the posted material.

Clickjacking: A malicious technique of tricking a user into revealing confidential information or taking control of their computer while clicking on seemingly harmless web pages. On a clickjacked page, the attacker shows a set of dummy buttons or links, then loads another page over it in a transparent layer. Users think they are clicking on the visible page while they are actually performing actions on the hidden page which the users never intended, such as changing privacy settings on a social networking site or following someone on Twitter.

Commercial/Third-Party Social Media: Social media hosted on servers over which DHS has no control. This includes proprietary social networking sites such as Facebook, MySpace, and Bebo, as well as collaboration services such as Wikipedia, BlogSpot, and Delicious.

Content: Information of any kind published to the web (including text, graphics, symbols, retrievable data, and presentation concepts).

Content Manager: Any individual designated to manage web content for the Secret Service. The duties of the Content Manager include ensuring compliance with accessibility standards for persons with disabilities. This individual is the primary point of contact for web issues.

Controlled Unclassified Information (CUI): A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 13526, but is (a) pertinent to the national interests of the United States or to the important interests of entities outside of the Federal Government; and (b) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination (which has been similarly identified as Sensitive But Unclassified (SBU)).

Facebook: A social networking site where individuals can create and customize their own profiles, and organizations can create their own pages, with photos, videos, and information about themselves, and send e-mails or instant messages with other members.

Federal Record: As defined in Federal law, a Federal record is all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency, as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of data in them. (See 44 USC 3301)

Foursquare: A location-based social networking website and application for mobile devices. Users "check in" or report their location by accessing a mobile website, text messaging or a device-specific application, so that their whereabouts can be discovered by others. Foursquare also incorporates elements of a game by awarding users points for being the first to visit a new place, and for adding new

information about the locations they visit.

Friending: To add someone as a friend on a social networking website.

Internet footprint: The collective activities and behaviors recorded as an individual interacts in a digital environment, including device usage, system logins and logouts, website visits, files, transmitted emails, and posted messages. "Passive footprints" are created when data is collected about individuals' activities without any deliberate action on their part, such as tracking which products customers are visiting on a vendor's website regardless of whether purchases occur. "Active footprints" are created when personal data is released intentionally by individuals for the purpose of sharing information with others online. Footprints are sometimes used as a rough measure of an individual's "web presence."

Keystroke loggers: Also called a "keylogger." It is a hardware device or program that monitors and records each keystroke a user types on a computing device's keyboard. Although sometimes used for legitimate purposes, such as diagnostics or monitoring a child's Internet activity, a more typical use of keystroke loggers is for the unauthorized capture of security credentials such as passwords and personal identification numbers.

LinkedIn: A business-oriented social networking site mainly used for professional networking.

Location Based Services (LBS)/Location Based Social Networks: These services and applications collect and use location data. They offer a wide range of functionality, including: providing maps and local information to users, allowing users to share their locations with their friends, allowing people to track other people such as their employees or children, using player location information in electronic games, and providing location-based advertisements. These services use a variety of technologies to acquire a user's location based on the current location of the user's cell phone, computer, or other device. Some devices, such as smartphones, may use more than one locating technology. Examples of geo-location services are Facebook Places, Foursquare, Google Latitude, Loopt, BrightKite, Citysense, and Gowalla.

Make PII Available: The term "make PII available" includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using the website or application. "Associate" can include activities commonly referred to as "friending," "following," "liking," joining a "group," becoming a "fan," and comparable functions. (See Office of Management and Budget (OMB) Memorandum M-10-23)

Malware: Derived from the phrase "malicious software," this term is a general reference to any program whose purpose is to cause harm to a computer system.

Metadata: Information about the meaning of other information. Metadata can describe or summarize key attributes of a piece of information to facilitate finding that information when needed. An example of metadata is a time stamp that specifies when a piece of information was created.

Micro-Blog: Extremely short blog posts similar to text messaging. The messages can either be viewed by anyone or by a restricted group that is chosen by the user. Twitter, a popular micro-blog client, allows for posts of up to 140 characters in length to be uploaded and read online through instant messaging or mobile devices via text messaging.

Personally Identifiable Information (PII): Any information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (See OMB M-07-16)

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing

this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual. (See OMB M-10-23)

Pharming: An action whereby a hacker subverts a user's attempt to visit a legitimate website by instead redirecting him or her to a counterfeit or "spoofed" website. The spoofed site is designed to trick users into revealing personal information such as usernames, passwords, and account information.

Phishing: An attempt to fraudulently acquire a user's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Phishing is common in e-mail and instant messaging.

Photo Sharing: Websites that allow users to post and share digital photos. These sites typically allow commenting and metadata to be attached to photos.

Privacy Impact Assessment (PIA): An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. (See NIST SP 800-53; OMB Memorandum M-03-22)

Privacy Notice: While a Privacy Policy is a statement about an agency's general practices, the term "Privacy Notice" refers to a brief description of how the agency's Privacy Policy will apply in a specific situation. Because the Privacy Notice should serve to notify individuals before they engage with an agency, a Privacy Notice should be provided on the specific web page or application where individuals have the opportunity to make PII available to the agency. (See OMB Memorandum M-10-23)

Privacy Policy: The term "Privacy Policy" is described in OMB Memorandum M-99-18, and is further explained in OMB Memorandum M-03-22. When the term is used in OMB Memorandum M-10-23, it refers to a single, centrally located statement that is accessible from an agency's official homepage. The Privacy Policy should be a consolidated explanation of the agency's general privacy-related practices that pertain to its official website and its other online activities. (See OMB Memorandum M-10-23)

Privacy Threshold Analysis (PTA): A PTA is required for every system. The PTA is used to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002. The PTA is used in the Capital Planning and Investment Control (CPIC) process, for Certification and Accreditations (C&A), and to assist in determining the Federal Information Processing Standards (FIPS) level of a system. (See http://www.dhs.gov/privacy)

Sensitive Personally Identifiable Information (PII): Personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines.

Examples of Sensitive PII include:

- Social Security number;
- Driver's license number;
- Financial account number or information;
- Biometric identifier (e.g., fingerprint, iris scan)
- Alien registration number (A-Number);
- Citizenship or immigration status;
- Medical information;
- Ethnic, religious, sexual orientation, or lifestyle information; and
- Account passwords.

Other PII may be "sensitive" depending upon its context, such as a list of employees with poor performance ratings. (See DHS Privacy Incident Handling Guidance)

Social Bookmarking: A web-based service where users create and store links. Although web browsers have the ability to bookmark pages, those links are tied to that browser on that computer. Social bookmarking, in contrast, is tied to an online account, which can be made public. These bookmarks can be shared and discovered by others. Examples of social bookmarking sites include Delicious, Digg, and Reddit.

Social Engineering: The act of manipulating people into performing actions or divulging confidential information through trickery or deception, rather than by breaking in or using technical means. For example, someone posing as a help desk representative might call you and claim to be diagnosing a connection problem and request that you verify your login ID and password or other personal information so it can be checked against the items on file.

Social Media: Internet-based applications that build on the foundations of Web 2.0 to allow the creation and exchange of user-generated content. Social media can take many different forms, including, but not limited to, web-based communities and hosted services, social networking sites, video and photo sharing sites, wikis, blogs, podcasts, virtual worlds, social bookmarking, and other emerging technologies.

Social Networking Services: Tools used to connect people who share the same interests and/or activities, or who are interested in exploring the interests and activities of others. Social network services are Internet-based and provide a variety of ways for users to interact. For example, Facebook is regarded as a place to socialize with friends, whereas LinkedIn caters to those who wish to make professional connections.

Spear Phishing: Spear phishing is an attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Spear phishers rely on knowing some personal piece of information about their target, such as an event, interest, travel plans, or current issues. Sometimes this information is gathered by hacking into the targeted network, but often it is easier to look up the target on a social media network. Social networking sites are used as a mechanism for attackers to gather information on their targets by harvesting information from publically accessible networks and using the information as an attack vector. Spear phishers use social media as an alternative way to send phishing messages, as the social media platform bypasses traditional e-mail security controls.

Terms of Service (ToS or TOS): Rules by which one must agree to abide by in order to use a service. Terms of service can cover a range of issues, including acceptable user behavior online, a company's marketing policies, and copyright notices. Some organizations can change their terms of service without notice to the user base.

Third-Party Websites or Applications: The term "third-party websites or applications" refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a non-government entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official website. (See OMB Memorandum M-10-23)

Trusted Internet Connection (TIC): A DHS Initiative, outlined in OMB Memorandum M-08-05, Implementation of Trusted Internet Connections, to optimize and standardize the security of individual external network connections, to include connections to the Internet, currently in use by the Federal Government. A "TIC" is a physical location an agency uses to meet the objective of the TIC Initiative. The Federal TIC program provides a series of inspection, monitoring, detection, and blocking technologies that ensure additional security and visibility to defend against a wide array of attacks, including those discussed from a social media perspective.

Twitter: A social networking micro-blogging service that enables its users to send and read other users' messages, called "tweets." Users ("followers") may subscribe to ("follow") other users' tweets. Twitter is sometimes called the "Short Message Service of the Internet" because of the compatibility of its interface with smartphones.

Uniform Resource Locator (URL): In computing, the identifier that specifies where a resource is located and the mechanism for retrieving it. The best-known example of the use of URLs is for the addresses of web pages on the Internet, such as www.dhs.gov.

YouTube: A video-sharing website on which users can upload, share, and view videos.

Virtual World: Online communities where users or their digital representations (called "avatars") can socialize, connect, and interact with one another using text and/or voice chat. The term is used more specifically to refer to an online community (such as Second Life) that features a computer-based simulated, three-dimensional environment where users not only can interact but also create and use objects.

Web 2.0: Web 2.0 technologies refer to a second generation of the World Wide Web as an enabling platform for web-based communities of interest, collaboration and interactive services. These technologies include web logs (known as "blogs"), which allow individuals to respond online to agency notices and other postings; social-networking sites (such as Facebook and Twitter), which also facilitate informal sharing of information among agencies and individuals; video-sharing websites (such as YouTube), which allow users to discover, watch, and share originally created videos; "wikis," which allow individual users to directly collaborate on the content of web pages; "podcasting," which allows users to download audio content; and "mashups," which are websites that combine content from multiple sources.

Whaling: Phishing attacks targeted at high-ranking personnel in the organizational hierarchy, such as Chief Executive Officers (CEO) and other top executives.

Widgets: A self-contained tool that can be embedded into a website or program to deliver a single-purpose service, such as displaying the latest news and weather, maps, photos, or allowing a user to play interactive games with other website visitors. Users of social networking sites often take advantage of widgets as an easy way to make their sites more interesting to visitors; however, care must be taken since they can be used as a malware entry point.

Wiki: A collection of web pages that encourages users to contribute or modify the content. By using a simple web interface, a community can collaborate on developing a document or web page, no matter where they are located.

DISCIPLINARY AND ADVERSE ACTIONS – GENERAL

Policy

Sections ITG-06(01) through ITG-06(07) contain policies and procedures for informal and formal disciplinary and adverse actions for employee misconduct and performance deficiencies. In order to accomplish the dual mission of the United States Secret Service (Secret Service), all employees are required to maintain high standards of honesty, integrity, and personal conduct. When these standards are not met, it is essential that prompt, corrective action is taken that promotes the efficiency of the service.

Authorities

- Title 5, United States Code (U.S.C.), Chapter 75, Adverse Actions.
- Title 5, U.S.C., Chapter 77, Appeals.
- Title 5, Code of Federal Regulations (C.F.R.), Part 752, Adverse Actions.
- Title 5, C.F.R., Chapter II, Merit Systems Protection Board.

Basic Principles

The Secret Service will adhere to job protection procedures required by the Office of Personnel Management (OPM), and Title 5, U.S.C., Chapter 75. Disciplinary and adverse actions shall be governed by the following principles:

1. **Consistent** - similar penalties should be imposed for like offenses, with due consideration given to mitigating or aggravating circumstances.

2. **Corrective** - the intent of discipline is not to punish, but to correct unacceptable behavior. Accordingly, a disciplinary or adverse action should only be as severe as is necessary to bring about the desired change.

3. **Nondiscriminatory** - disciplinary and adverse actions shall not be influenced by the race, color, religion, national origin, disability (physical or mental), gender, age, sexual orientation, genetic information, parental status of an employee, partisan political reasons, veterans' status, marital status, or in reprisal for opposing discrimination or prior participation in the Equal Employment Opportunity (EEO) process.

4. **Timely** - disciplinary and adverse actions will be initiated as soon as practicable after management becomes aware of the misconduct, or the Office of Integrity and the appropriate Assistant Director is provided with a completed report of investigation concerning the misconduct.

5. **Progressive** - a more severe adverse action than would otherwise be taken may be imposed upon an employee when that employee has previously received discipline. The prior offense(s) need not have been of the same nature as the current offense(s) in order to warrant a more severe action. The concept of progressive discipline does not preclude removal as a penalty for a first offense in those cases where employee misconduct is so serious as to warrant it. The concept of progressive discipline does not mean that a second disciplinary action must be more severe than the first disciplinary action. Rather, a disciplinary or adverse action for a second offense should be more severe than would otherwise have been issued for an initial offense of that same nature.

6. **Constructive** - all disciplinary and adverse actions must be taken for good cause.

7. **Effect on the Federal Service** - disciplinary or adverse actions should be taken only for such cause as promotes the efficiency of the Federal service, and only in those cases where there is a nexus between the offense and the employee's duties or position.

Definitions

The following should be reviewed as an aid to understanding disciplinary and adverse actions:

1. **Adverse Action –** removal, reduction in pay, or a suspension of any length.

2. **Discipline Review Board (DRB) –** a collateral duty board made up of a representative, at the Deputy Assistant Director or Deputy Chief level or above, from each Assistant Director's office and the Uniformed Division (with the exception of the Office of the Chief Counsel and the Office of Professional Responsibility). An attorney from the Office of the Chief Counsel and a representative from the Office of Integrity will act as advisory members to the DRB. If the employee who is the subject of the disciplinary or adverse action is assigned to Office of the Chief Counsel, the Office of Professional Responsibility, or the Office of the Director, an employee from that office who is at the GS-15 level or above will also serve as a member of the DRB. Once the DRB is convened, to the extent practicable, the members of the DRB shall remain unchanged for a one year period.

3. **Douglas Factors –** The Merit Systems Protection Board in its landmark decision, *Douglas vs. Veterans Administration*, 5 M.S.P.R. 280 (1981), established criteria that supervisors must consider in determining an appropriate penalty to impose for an act of employee misconduct. The criteria, which became known as the Douglas Factors, are:

    1) The nature and seriousness of the offense, and its relation to the employee's duties, position, and responsibilities, including whether the offense was intentional or technical or inadvertent, or was committed maliciously or for gain, or was frequently repeated;

    2) The employee's job level and type of employment, including supervisory or fiduciary role, contacts with the public, and prominence of the position;

    3) The employee's past disciplinary record;

    4) The employee's past work record, including length of service, performance on the job,

ability to get along with fellow workers, and dependability;

5) The effect of the offense upon the employee's ability to perform at a satisfactory level and its effect upon supervisors' confidence in the employee's ability to perform assigned duties;

6) Consistency of the penalty with those imposed upon other employees for the same or similar offenses;

7) Consistency of the penalty any applicable agency table of penalties;

8) The notoriety of the offense or its impact upon the reputation of the agency;

9) The clarity with which the employee was on notice of any rules that were violated in committing the offense, or had been warned about the conduct in question;

10) The potential for the employee's rehabilitation;

11) Mitigating circumstances surrounding the offense such as unusual job tensions, personality problems, mental impairment, harassment, or bad faith, malice or provocation on the part of others involved in the matter; and

12) The adequacy and effectiveness of alternative sanctions to deter such conduct in the future by the employee or others.

4. **Employee at the GS-15 Level or Below** – all Secret Service employees who are not members of the Senior Executive Service, to include Senior Leaders and all Uniformed Division Officers, Sergeants, Inspectors, Captains, Lieutenants, Assistant Chiefs, and Deputy Chiefs. The Chief of the Uniformed Division will be considered to be above the GS-15 level for purposes of this policy.

5. **Expiration of Appointment** – termination of employment on a date set at time of appointment to federal service.

6. **Formal Discipline** – a written reprimand.

7. **Grade** – a level of classification under a position classification or job grading system.

8. **Indefinite Suspension** – the placement of an employee in a temporary status without duties or pay pending investigation, inquiry, or other further action. An indefinite suspension must have at least one previously identified condition, that, when met, will terminate the suspension.

9. **Informal Discipline** – verbal counseling or memorandum of counseling.

10. **Intake Group** – the intake group is made up of the Chief of the Security Clearance Division or higher; the Deputy Chief Integrity Officer; an attorney from the Office of the Chief Counsel; a representative from the Inspection Division; and a representative from the affected employee's Assistant Director's office. The representatives will be at the GS-15 level or higher. The representative from the affected employee's Assistant Director's office cannot serve as a representative on both the Intake Group and the Discipline Review Board for the same case.

11. **Pay** – the rate of basic pay fixed by law or administrative action for the position held by an employee before any deductions, and exclusive of additional pay of any kind. For the purposes of this chapter, pay does not include locality-based comparability payments, or other similar payments; however, it does include Law Enforcement Availability Pay (LEAP).

12. **Preference Eligible Employee –** an individual entitled to veterans' preference pursuant to 5 U.S.C. § 2108. Generally, this includes employees who: (1) served on active duty in the armed forces during a war, or in a campaign or expedition for which a campaign badge has been authorized, or during the period from April 28, 1952 to July 1, 1955; (2) served on active duty at any time in the armed forces for a period of more than 180 days during the period from January 31, 1955 to October 15, 1976, or from September 11, 2001 to the date prescribed by Presidential proclamation or by law as the last date of Operation Iraqi Freedom; or (3) served on active duty in the armed forces from August 2, 1990 to January 2, 1992. "Active duty" is defined by 38 CFR § 101(21). Employees may also be entitled to veterans' preference if they are a disabled veteran. Under limited circumstances, certain family members of deceased veterans, or family members of veterans who, because of a service connected disability, are unable to qualify for civil service appointment, may also be entitled to veterans' preference.

13. **Probationary Period –** is defined in 5 CFR § 315.801 as generally the first year of service of an employee who is appointed to a position in the competitive service.

14. **Removal –** the involuntary separation of an employee from employment with the Secret Service and from Federal service.

15. **Reprimand –** a memorandum of official censure for a serious violation of a rule of conduct, law, regulation, official instruction, or specified responsibility for which a more severe disciplinary action is not warranted.

16. **Similar positions –** positions in which the duties performed are similar in nature and character and require substantially the same or similar qualifications so that the incumbent could be interchanged between the positions without significant training or undue interruption to the work.

17. **Suspension** – the placement of an employee in a temporary status without duties or pay for disciplinary reasons and for a set period of time.

18. **Table of Offense Codes and Penalty Guidelines ("Table of Penalties") –** a list of Offense Codes and Penalty Guidelines which serve as a guide in determining appropriate corrective, disciplinary, or adverse actions for common offenses; and which supersedes all previous policies and practices regarding disciplinary offenses and penalties. The Offense Codes provide a general description of certain types of misconduct and do not cover all possible offenses. Offenses not described in the Offense Codes may be separately identified and result in appropriate disciplinary or adverse action, provided there is a nexus between the misconduct and the efficiency of the service. The Penalty Guidelines provide the range of disciplinary action, along with mitigating and aggravating factors.

19. **Trial Period –** is the excepted service hiring authority equivalent of the probationary period. During this time, employees are provided developmental opportunities and assessed for skills. The length of the trial period is determined by the type of excepted service hiring authority.

Responsibilities

The Director, Deputy Director, Assistant Directors (ADs), Chief Counsel, and Chief of the Uniformed Division have authority and responsibility for:

1. Ensuring that disciplinary and adverse actions policies and procedures are effectively applied and administered;
2. Assuring the proper training of supervisors in matters relating to disciplinary or adverse actions, and appeals;
3. Promptly reporting allegations of misconduct to the Office of Professional Responsibility, Inspection Division; and,
4. Proposing and taking disciplinary and adverse actions where a Senior Executive Service (SES) level employee is the subject of the action.

The Office of Professional Responsibility, Inspection Division, is responsible for:

1. Convening and chairing the Intake Group when an allegation of misconduct has been received;
2. Conducting investigations into allegations of employee misconduct;
3. Preparing reports of investigations; and
4. Providing a copy of investigative report(s) to the Office of Integrity for further action as appropriate.

The Intake Group is responsible for:

1. Reviewing all allegations of misconduct received by the Office of Professional Responsibility and determining whether further investigation by the Inspection Division is warranted;
2. Referring allegations of misconduct where additional investigation is not warranted to the Office of Integrity for appropriate administrative action;
3. Administratively closing cases where allegations of misconduct are unfounded, lacking in specificity, or where no violation of Secret Service policy has occurred;
4. Notifying the Office of Integrity and the appropriate Assistant Director or Chief Counsel when a matter is referred to the Inspection Division; and,
5. Referring matters to the appropriate Assistant Director or Chief Counsel for informal disciplinary action when appropriate.

The Office of Integrity is responsible for:

1. Preparing and issuing the written notice of the disciplinary or proposed adverse action and decision documents (including the preparation of files and memoranda relating to disciplinary and adverse actions, appeals, and grievances). The Deputy Chief Integrity Officer will be the issuing official for reprimands and will be the proposing official for all adverse actions. The Chief Integrity Officer will be the deciding official for all adverse actions;
2. Consulting with the Office of the Chief Counsel in all adverse action cases. The staff of the Office of Integrity will also consult with the Office of the Chief Counsel in other appropriate cases, for example, where the alleged misconduct could result in claims such as discrimination, or may constitute protected disclosures under the Whistleblower Protection Act;
3. Providing advice and guidance to the DRB in the area of disciplinary and adverse actions, grievances, and appeals; and
4. Providing a representative at the GS-15 level (other than the Chief Integrity Officer or Deputy Chief Integrity Officer) to the DRB, who will serve as the clerk of the DRB. As the clerk of the DRB, the GS-15 representative will call the meetings, set the agenda, prepare a summary of the DRB's proceedings, and otherwise facilitate the operation of the DRB.

The Office of the Chief Counsel is responsible for:

1. Providing legal advice, consultation, drafting and review, in regard to all disciplinary and adverse actions, grievance, appeals, and reviews.

The Discipline Review Board (DRB) is responsible for:

1. Deciding employee grievances for disciplinary actions or suspensions of 14 days or less based on the record of the case and the employee's written grievance request;
2. Deciding non-SES level employee grievances of suspensions of more than 14 days, and reductions in grade or pay, or removals where the employee has waived his/her Merit Systems Protection Board (MSPB) appeal rights. The DRB's decision will be based on the record of the case and the employee's written appeal. An employee may request a personal appearance before the DRB at his/her own expense; and,
3. Consulting with the Office of the Chief Counsel prior to issuing a decision on employee grievances, and seeking review by the Office of the Chief Counsel of all written decisions and correspondence concerning the DRB's actions.

Supervisors are responsible for:

1. Promptly reporting allegations of misconduct;
2. Administering informal disciplinary actions upon referral from the Intake Group or the Office of Integrity;
3. Ensuring that employees are not scheduled to work scheduled overtime in the same pay period in which they are suspended;
4. Ensuring that employees' time and attendance records, when appropriate, are properly documented as "Suspension;" and,
5. Ensuring adherence to all other statutory and regulatory procedural requirements.

From: HUM
Sent: Friday, October 30, 2015 3:15 PM
To: USA
Cc: HUM
Subject: DCP#: HRT 2015-55, DIR 2015-08 Whistleblower Protection Awareness

//ROUTINE//

FROM: Headquarters (AD - Human Resources) DCP#: HRT 2015 - 55
DIR 2015 - 08

TO: All Supervisors and Holders of the Human Resources and Training Manual
All Holders of the Office of the Director Manual
All Employees

SUBJECT: Whistleblower Protection Awareness

This directive should be reproduced locally and filed in front of the following Secret Service manual sections:

- Human Resources and Training Manual section HCD-05, "Your Rights as a Federal Employee."
- Office of the Director Manual section ITG-03(04), "Department Wide Employee Rules of Conduct."

This directive is in effect until superseded.

The Secret Service, along with the Department of Homeland Security (DHS), is committed to protecting the rights of employees who report what they reasonably believe are violations of law, rule, or regulation, gross mismanagement, gross waste of funds, abuse of authority, or substantial and specific danger to public health and safety. By unifying efforts with employees and citizens, the Department, the DHS Office of Inspector General, and the U.S. Office of Special Counsel aim to protect the integrity, effectiveness, and efficiency of all DHS programs.

The Department is pursuing certification of whistleblower protections from the U.S. Office of Special Counsel. As part of the certification process, by close of business on November 3, 2015, the following posters must be printed and displayed in all office areas where employee notices are posted. For any poster that is currently displayed in the office, check the revision date in the lower right corner to ensure the most recent poster is displayed. To download a copy of each of the posters listed below, hover over the link, hold the Ctrl button down and left click (or copy the Web address into your browser).

- DHS_OIG_Hotline_Poster
https://www.oig.dhs.gov/assets/Hotline/DHS_OIG_Hotline-optimized.jpg

- Prohibited Personnel Practices Poster
  https://osc.gov/Resources/PPP%20Poster%20Update.pdf

- Whistleblower Retaliation Poster
  https://osc.gov/Resources/post_wbr.pdf

- Hatch Act - Further Restricted Employees Poster
  https://osc.gov/Resources/HA%20Poster%20_Further%20Restricted%20Employees%20-%20with%20OSC%20contact%20info%20(5-11).pdf

Other helpful resources can be found on the DHS Whistleblower Protection Web site.
(http://dhsconnect.dhs.gov/org/comp/mgmt/Pages/Whistleblower-Protection.aspx).

This site provides information to help employees easily determine what they should report, how to report suspected issues, what training DHS offers, what legal protections are available, in addition to a number of other helpful tools and guidance.

Headquarters (Human Resources) Triplett

United States Secret Service
Directives System

Manual : Human Resources and Training
RO : HCD

Section : HCD-05
Date : 12/01/2014

Subject: Your Rights as a Federal Employee (and Migration of Employee Responsibilities and Conduct Policy to the Office of the Director Manual)

To: All Supervisors and All Manual Holders of the Human Resources and Training Manual

Filing Instructions:

- Remove and destroy the Human Capital Division (HCD) Numbering Conversion in its entirety and replace with the attached updated HCD Numbering Conversion.
- Remove and destroy PER-05 in its entirety, **except for PER-05(06), which should remain in place.**
- File the attached section HCD-05, followed by the attached PER-05(01) through PER-05(05) slipsheets, immediately in front of PER-05(06).
- File this Policy Memorandum in front of HCD-05.
- This directive is in effect until superseded.

Impact Statement: This directive formalizes the migration of Employee Responsibilities and Conduct policy from the Human Resources and Training Manual to the Integrity chapter, section ITG-03, within the Office of the Director Manual. (See DCP# DIR 2014-03).

This directive also updates policy regarding Your Rights as a Federal Employee to incorporate current guidance issued by the U.S. Office of Special Counsel (OSC), and establishes coverage of that subject under HCD-05.

Policy regarding Outside Employment, which will remain in PER-05(06) on an interim basis, will be revised in the near future and incorporated into a corresponding directive.

Mandatory Review: The Responsible Office will review all policy contained in this section in its entirety by or before December 2018.

Questions regarding this policy may be directed to the Human Capital Division, Employee Relations Branch, at 202-406-5670.

Victor Erevia
AD - Human Resources and Training

DCP#: HRT 2014-65

YOUR RIGHTS AS A FEDERAL EMPLOYEE

Introduction

The purpose of this policy is to ensure that all Secret Service employees are aware of and understand the prohibited personnel practices and whistleblower protections available to Federal employees.

The December 5, 2013, White House National Action Plan calls for covered agencies to certify compliance with the Whistleblower Protection Act's notification requirements. To that end, this policy provides links to information about the U.S. Office of Special Counsel (OSC), which is an independent agency that protects Federal employees from prohibited personnel practices, including whistleblower retaliation and unlawful hiring practices. OSC also provides an independent, secure channel for disclosing and resolving wrongdoing in Federal agencies.

The Whistleblower Protection Act of 1989 and the Whistleblower Protection Enhancement Act of 2012 provide the right for all covered Federal employees to make whistleblower disclosures and ensure that employees are protected from whistleblower retaliation. Whistleblowing is defined as the disclosure of information that an employee reasonably believes evidences: a violation of any law, rule or regulation; gross mismanagement; gross waste of funds; an abuse authority; a substantial and specific danger to public health or safety; or censorship related to scientific research or analysis. Employees may make lawful disclosures to anyone, including, for example, management officials, the Inspector General of an agency, and/or OSC.

The pages which follow outline the role of the U.S. Office of Special Counsel, and describe the processes for making whistleblower disclosures and/or prohibited personnel practices complaints by Federal employees. They summarize materials and resources that may be accessed directly via the OSC web site at http://osc.gov.

All employees also are encouraged to review "Your Rights as a Federal Employee," which provides detailed information on the thirteen prohibited personnel practices and employees' rights to file complaints with OSC. A copy is included at the end of this section, and is also available at the following url: https://osc.gov/Resources/Your Rights as a Federal Employee.pdf.

In addition, a pamphlet entitled "Know Your Rights When Reporting Wrongs" describes different avenues for making whistleblower disclosures and OSC's role in accepting complaints from Federal employees. This pamphlet is likewise included at the end of this section, and can also be accessed via the OSC web site at https://osc.gov/Resources/Know Your Rights When Reporting Wrongs.pdf.

Federal employees have the right to be free from prohibited personnel practices, including retaliation for whistleblowing. The Secret Service is committed to making sure that all employees are aware of their rights as well as the safeguards that are in place to protect them.

Responsibilities

For detailed employee responsibility and standards of conduct policies related to this topic, see Office of the Director Manual section ITG-03, "Employee Responsibilities and Conduct."

The Role of the U.S. Office of Special Counsel

The U.S. Office of Special Counsel (OSC) is an independent federal investigative and prosecutorial agency. Under the Civil Service Reform Act and the Whistleblower Protection Act, the OSC's primary mission is to safeguard the merit system by protecting federal employees and applicants from prohibited personnel practices, especially reprisal for whistleblowing.

The OSC is responsible for facilitating disclosures of wrongdoing in the federal government. It also has jurisdiction under the Hatch Act to enforce restrictions on political activity by government employees.

Finally, the OSC participates in enforcement of the Uniformed Services Employment and Reemployment Rights Act.

The OSC carries out its mission by:

- investigating allegations of prohibited personnel practices and other improper employment practices within its jurisdiction, and seeking any appropriate corrective or disciplinary action;
- providing an independent, secure channel for disclosure and resolution of wrong doing in federal agencies;
- interpreting and enforcing Hatch Act provisions on permissible and impermissible political activity;
- promoting greater understanding of the rights and responsibilities of government employees; and
- enforcing the law that protects service members reemployment rights.

Investigating and Prosecuting Prohibited Personnel Practices

What are "prohibited personnel practices?"

Prohibited personnel practices, including reprisal for whistleblowing, are defined by law at § 2302(b) of title 5 of the United States Code (U.S.C.). A personnel action (such as an appointment, promotion, reassignment, or suspension) may need to be involved for a prohibited personnel practice to occur. Generally stated, § 2302(b) provides that a federal employee authorized to take, direct others to take, recommend or approve any personnel action may not:

1. discriminate against an employee or applicant based on race, color, religion, sex, national origin, age, handicapping condition, marital status, or political affiliation;
2. solicit or consider employment recommendations based on factors other than personal knowledge or records of job-related abilities or characteristics;
3. coerce the political activity of any person;
4. deceive or willfully obstruct anyone from competing for employment;

5. influence anyone to withdraw from competition for any position so as to improve or injure the employment prospects of any other person;

6. give an unauthorized preference or advantage to anyone so as to improve or injure the employment prospects of any particular employee or applicant;

7. engage in nepotism (i.e., hire, promote, or advocate the hiring or promotion of relatives);

8. engage in reprisal for whistleblowing—i.e., take, fail to take, or threaten to take or fail to take a personnel action against an employee or applicant for disclosing to the Special Counsel, or to an Inspector General or comparable agency official (or others, except when disclosure is barred by law, or by Executive Order to avoid harm to the national defense or foreign affairs) information which the employee or applicant reasonably believes evidences a violation of any law, rule or regulation; gross mismanagement; a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety;

9. take, fail to take, or threaten to take or fail to take a personnel action against an employee or applicant for exercising an appeal, complaint, or grievance right; testifying for or assisting another in exercising such a right; cooperating with or disclosing information to the Special Counsel or to an Inspector General; or refusing to obey an order that would require the individual to violate a law;

10. discriminate on the basis of off-duty conduct which does not adversely affect job performance;

11. take or fail to take, recommend, or approve a personnel action, if taking or failing to take the action would violate a veterans' preference requirement;

12. take or fail to take a personnel action, if taking or failing to take the action would violate any law, rule, or regulation implementing or directly concerning merit system principles at 5 U.S.C. §2301; or

13. implement or enforce a nondisclosure agreement or policy lacking notification of whistleblower rights.

Who can be protected by the OSC from prohibited personnel practices?

The OSC has jurisdiction over prohibited personnel practices committed against most employees or applicants for employment in Executive Branch agencies and the Government Printing Office, but not against employees of:

- the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, and certain other intelligence agencies excluded by the President;
- The armed forces of the United States (i.e., uniformed military employees);
- the Government Accountability Office;
- the U.S. Postal Service and Postal Rate Commission;
- the Federal Bureau of Investigation; and
- government corporations. (Note, however, that employees and applicants in government corporations listed at 31 U.S.C. § 9101 are covered by statutory whistleblower protections.)

How does the OSC handle a prohibited personnel practice complaint?

Complaints Examining Unit (CEU). The CEU receives complaints filed with the OSC. (Procedures for filing prohibited personnel practice and other complaints are described on the OSC web site). The unit analyzes all allegations of prohibited personnel practices (as well as allegations of other activities prohibited by civil service law, rule or regulation).

When necessary, a CEU examiner contacts the complainant to ensure that the examiner clearly understands the nature of and basis for each allegation. The examiner conducts further inquiry to the extent necessary to determine whether each allegation warrants additional investigation.

Persons who have submitted allegations to the CEU will receive:

- a letter acknowledging receipt of their complaint and identifying the staff member assigned to handle it, with information enclosed about how the complaint will be processed by the CEU; and
- a status report after 90 days, and every 60 days thereafter while the matter is active; and
- a letter advising that the matter has been referred to the OSC Investigation Division for further inquiry, with information enclosed about Investigation Division processes; or
- a preliminary letter, with a final opportunity for input when the CEU proposes to close a matter without remedial action or referral to the Investigation and Prosecution Division; or
- a letter advising that the OSC will take no further action because it lacks jurisdiction over the matter.

The OSC asks everyone who seeks an investigation of a possible prohibited personnel practice to select one of three consent statements explaining necessary communications between OSC and the agency involved. (Consent statements are shown at the OSC's Internet home page at www.osc.gov.)

Alternative Dispute Resolution (ADR) Unit. After CEU has completed its examination, OSC offers mediation, as an alternative to investigation, in selected prohibited personnel cases. Participation in the OSC mediation program is completely voluntary for both the complainant and the agency. If both parties agree to mediate their dispute, the OSC assigns a neutral third party - a mediator - to facilitate a discussion between the parties to reach a mutually agreeable resolution to the complaint. For more information on mediation at the OSC, click on the Mediation Program link on the OSC Web site at www.osc.gov (under Forms and Publications), or request a Mediation Program brochure from the OSC ADR Unit.

Investigation and Prosecution Division (IPD). After a thorough initial examination, the CEU refers matters indicating a potentially valid claim (under the laws enforced by the OSC) to OSC's Investigation and Prosecution Division Unit. This unit conducts investigations to review pertinent records and to interview complainants and witnesses with knowledge of the matters alleged. Matters not resolved during the investigative phase will undergo legal review and analysis to determine whether the IPD inquiry has established a violation of law, rule or regulation and whether the matter warrants corrective action, disciplinary action or both. Complainants will continue to receive 60-day status notices while matters are pending in the division.

Can the OSC delay a personnel action pending investigation of the matter?

An individual may request that the Special Counsel seek to delay, or "stay," an adverse personnel action pending an OSC investigation. OSC will consider requesting a stay of a personnel action against an employee from an agency or from the U.S. Merit Systems Protection Board (MSPB) where: OSC has reasonable grounds to believe that a personnel action which was taken or will be taken constitutes a prohibited personnel practice and without a stay the employee will be subjected to removal; a suspension for more than 14 days; a reduction In grade; a significant reduction In pay; a geographic reassignment; the non-renewal of an appointment or another personnel action which the complainant demonstrates will result in a serious, immediate hardship or where there exists a substantial likelihood a personnel action was taken or is to be taken, as a result of a prohibited personnel practice or where Special Counsel, in his sole discretion, otherwise determines that it would be appropriate and consistent with OSC's statutory mission to request a stay from the MSPB. If the agency does not agree to a delay, the OSC may then ask the MSPB to stay the action. (The OSC cannot stay a personnel action on its own authority.)

How can the OSC remedy a prohibited personnel practice?

General. Current and former federal employees and applicants for federal employment may report suspected prohibited personnel practices to the OSC (see p. 15 for details). The matter will be investigated, and if there is sufficient evidence to prove a violation, the OSC can seek corrective action, disciplinary action, or both. Alternatively, parties in selected cases may agree to mediate their dispute in order to reach a mutually agreeable resolution of the prohibited personnel practice complaint.

Corrective action. The OSC may enter into discussions with an agency at any stage of a pending matter in pursuit of a resolution acceptable to all parties. The OSC follows a policy of early and firm negotiation to obtain appropriate corrective action (and/or disciplinary action) for apparent violations. If an agency fails to remedy a prohibited personnel practice upon request by the OSC, corrective action may also be obtained through litigation before the MSPB. Such litigation begins with the filing of a petition by the OSC, alleging that there are reasonable grounds to believe that a prohibited personnel practice has occurred, exists, or is about to occur.

Corrective actions that can be ordered by the MSPB include job restoration, reversal of suspensions and other adverse actions, reimbursement of attorney's fees, back pay, and medical and other costs and damages.

How are allegations of whistleblower retaliation remedied?

The Whistleblower Protection Act also allows current or former federal employees and applicants for employment who allege that they were subjected to any personnel action because of whistleblowing to seek corrective action in an appeal to the MSPB. Such an appeal is known as an "individual right of action" (IRA).

By law, the employee or applicant must seek corrective action from the OSC before filing an IRA. The IRA may be filed:

- after the OSC closes a matter in which reprisal for whistleblowing has been alleged; or
- if the OSC has not notified the complainant within 120 days of receiving an allegation of whistleblower reprisal that it will seek corrective action.

A federal employee or applicant for employment engages in whistleblowing when the individual discloses to the Special Counsel or an Inspector General or comparable agency official (or to others, except when disclosure is barred by law, or by Executive Order to avoid harm to the national defense or foreign affairs) information which the individual reasonably believes evidences the following types of wrongdoing:

- a violation of law, rule, or regulation; or
- gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

Procedures for filing an IRA are set forth in MSPB regulations at 5 C.F.R. Part 1209. (In considering an IRA, it should be noted that the MSPB may refuse to take jurisdiction over any matters not specifically raised before the OSC.)

Disciplinary action. The OSC may seek disciplinary action against any employee believed to be responsible for committing a prohibited personnel practice. The OSC begins a disciplinary action case by filing a complaint with the MSPB, charging an employee with the commission of a prohibited personnel practice, and seeking disciplinary action against that person. Rights of employees against whom the OSC seeks disciplinary action in these cases are set forth in MSPB regulations, at 5 C.F.R. Part 1201, Subpart D.

In the alternative, at any time during its investigation of a matter, the OSC may authorize the agency involved to take disciplinary action against an employee believed to be responsible for committing a prohibited personnel practice. (Pursuant to 5 U.S.C. § 1214(f), during any OSC investigation under title 5, an agency may not take disciplinary action against any employee for any alleged prohibited activity under investigation, or for any related activity, without approval from the OSC.)

Intervention. Pursuant to 5 U.S.C. § 1212(c), the Special Counsel may intervene as a matter of right, or otherwise participate in most proceedings before the MSPB. The Special Counsel may not intervene in certain proceedings (IRAs brought under 5 U.S.C. § 1221, or matters otherwise appealable to the MSPB under 5 U.S.C. § 7701) without the consent of the person initiating the proceedings.

Can employees seek relief from the OSC for a prohibited personnel practice if they are covered by a collective bargaining agreement?

Pursuant to 5 U.S.C. § 7121(g), employees covered by a collective bargaining agreement must choose one of three avenues: an OSC complaint, an MSPB appeal, or a grievance under the collective bargaining agreement.

What is the OSC's policy about allegations of discrimination under § 2302(b)(1)?

Race, color, religion, sex, national origin, age, handicapping condition. The OSC is statutorily authorized to investigate allegations of discrimination based on race, color, religion, sex, national origin, age, or handicapping condition (see (1) under "What are prohibited personnel practices?", above). However, procedures for investigating such complaints have already been established in federal agencies and the Equal Employment Opportunity Commission (EEOC).

Therefore, to avoid duplicating those investigative processes, the OSC follows a general policy of deferring complaints involving discrimination to those agencies' procedures.

Marital status, political affiliation. Allegations of discrimination based on marital status, and political affiliation are not within the jurisdiction of the EEOC. Such allegations, however, may be prohibited personnel practices or other violations of law subject to investigation by the OSC.

Discrimination Under § 2302(b)(10), For Off-Duty Conduct, Can Also Be Investigated By OSC.

For example, Jack's employment is terminated because he attended a "Gay Pride" march; or he attended a "Pro-Life" event; or he attended an animal rights rally; or he attended a gun-owners' rights meeting.

What do I do if I believe my veterans' preference rights were violated?

You should file a complaint with U.S. Department of Labor, Veterans Employment and Training Service.

The Veterans Employment Opportunities Act of 1998 (VEOA), 5 U.S.C. § 3330 et seq., created a new avenue of administrative redress specifically for a preference eligible who alleges that a federal agency violated such individual's rights under any statute or regulation relating to a veterans' preference eligible.

Under the VEOA, in order to seek corrective action, a preference eligible is to file a written complaint with the U.S. Department of Labor, Veterans Employment and Training Service (VETS), **within 60 days** of the alleged violation. VEOA requires the Secretary of Labor, through VETS to investigate the complaint and, upon determining that a violation occurred, to attempt to resolve the complaint by making reasonable efforts to ensure that the agency complies with the statute or regulation relating to veterans' preference. If the Secretary is unable to resolve a complaint within 60 days, the Secretary is to provide notification of an unsuccessful effort to resolve the complaint to the complainant.

In light of the VEOA, OSC does not investigate allegations of violations of veterans' preference rights for corrective action purposes. (We still investigate such allegations for possible disciplinary action, however.) Thus, you should file a complaint alleging a violation of a veterans' preference rights with VETS, not OSC.

Additional information about VETS can be found at http://www.dol.gov/dol/vets.

What other violations does the OSC have jurisdiction to investigate?

Pursuant to 5 U.S.C. § 1216, the OSC may also investigate and seek appropriate corrective and disciplinary action for—

- activities prohibited by any civil service law, rule, or regulation (including any activity relating to political intrusion in personnel decision making);
- arbitrary or capricious withholding of information under the Freedom of Information Act; and
- involvement by any employee in any prohibited discrimination found by a court or administrative authority to have occurred in the course of any personnel action. The OSC is also authorized by 38 U.S.C.§4324 to investigate and litigate cases referred by the Department of Labor, involving the reemployment rights of veterans and reservists returning to the federal workplace after active duty.

Are Federal employees required to cooperate with OSC investigations?

Federal employees are required by Civil Service Rule 5.4 to provide to the OSC any information, testimony, documents, and material, the disclosure of which is not otherwise prohibited by law or regulation, in investigations of matters under civil service law, rule, or regulation. The same rule requires federal agencies to make employees available to testify, and to provide pertinent records to the OSC.

Title 5 of the U.S. Code authorizes the OSC to issue subpoenas for documents and the attendance and testimony of witnesses. During an investigation, the OSC may require employees and others to testify under oath, sign written statements, or respond formally to written questions.

What legal responsibilities do federal agencies have to prevent prohibited personnel practices?

Section 2302(c) of title 5 requires federal agency heads, and officials with delegated authority for any aspect of personnel management, to:

- prevent prohibited personnel practices, including reprisal for whistleblowing;
- comply with and enforce civil service laws, rules and regulations; and
- ensure (in consultation with the OSC) that federal employees are informed of their rights and remedies. The OSC has developed easy-to-use information and training guide for use by agencies in carrying out the duty of informing employees of their rights and remedies under title 5 (see p. 19 for information on availability). On request, the OSC may also make its personnel available to assist in conducting such training.

Receiving Whistleblower Disclosures

Who can use the OSC's whistleblower disclosure channel?

Current and former federal employees and applicants for employment can confidentially report wrongdoing in federal agencies to the OSC. The OSC serves as a secure channel that can be used to disclose a violation of any law, rule, or regulation; gross mismanagement; a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety. Whistleblower disclosures to the OSC must be made in writing. Such information can be reported to the OSC without fear of reprisal, or disclosure of the source's identity without that person's consent.

How are whistleblower disclosures handled by the OSC?

The OSC is not authorized to investigate allegations reported through its whistleblower disclosure channel. However, the OSC can require the head of the agency concerned to investigate the matter if the OSC determines that there is a substantial likelihood that the information discloses a violation of any law, rule, or regulation; gross mismanagement; a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety. In these cases, the head of the agency is required to submit a report of the agency's findings to the OSC. By law, employees or applicants may review and comment on agency reports resulting from information disclosed by them to the OSC. Their comments, together with any comments or recommendations by the Special Counsel, are sent with the agency report to the President and appropriate congressional oversight committees. The agency report is also made available to the public, as required by law.

Advising On and Enforcing The Hatch Act

What is the Hatch Act?

The Hatch Act governs political activity by government employees at the federal, state and local levels. Under amendments enacted by Congress in 1993, most federal and District of Columbia (D.C.) government employees are permitted (with significant limitations) to take an active part in partisan political management and campaigns. On December 19, 2012, Congress passed the Hatch Act Modernization Act of 2012, which allows most state and local government employees to run for partisan political office. However, certain federal agencies and categories of employees continue to be prohibited from taking an active part in partisan political management and partisan campaigns.

The Hatch Act also restricts political activity by certain state or local government employees employed in connection with programs financed by federal funds. These employees are not permitted to coerce the political activities of others, or to be candidates for public office in partisan elections.

Guidance on permissible social media activities under the Hatch Act, both for "less restricted" employees and for "further restricted" employees can be found on the OSC web site at www.osc.gov.

What is the OSC's role?

The OSC is authorized by law to provide Hatch Act advisory opinions. These opinions respond to questions from government employees and others about whether or not they may engage in specific political activities under the act.

The OSC also enforces Hatch Act provisions on permissible and impermissible political activity by government employees. It is the only agency authorized to prosecute violations of the act, which are adjudicated by the MSPB.

An employee who violates the Hatch Act is subject to a range of disciplinary actions, including removal from federal service, reduction in grade, debarment from federal service for a period not to exceed 5 years, suspension, letter of reprimand, or a civil penalty not to exceed $1,000.

What restrictions apply to employees of the Federal government and the District of Columbia?

Under the Hatch Act, as amended (5 U.S.C. §7321, et seq.), most federal and D.C. government employees (with certain exceptions noted) may take an active part in partisan political management and campaigns. They may:

- be candidates for public office in nonpartisan elections;
- register and vote as they choose;
- assist in voter registration drives;
- express opinions about candidates and issues;
- contribute money to political organizations;
- attend political fundraising functions;
- attend and be active at political rallies and meetings;
- join and be active members of political parties and clubs;
- sign nominating petitions;
- campaign for or against referendum questions, constitutional amendments, or municipal ordinances;
- campaign for or against candidates in partisan elections;
- make campaign speeches for candidates in partisan elections;
- distribute campaign literature in partisan elections; and
- hold office in political parties or clubs.

There continues to be important restrictions on employees' political activity. Whether on-duty or off-duty, employees may **not:**

- use their official authority or influence to interfere with or affect the result of an election;
- solicit, accept or receive political contributions from anyone (with a very narrow exception in certain circumstances for solicitations of other federal employees for contributions to federal labor organizations and certain other employee organizations);
- knowingly solicit or discourage political activity of anyone who has business before their agency;
- run for public office in a partisan political election.

Except for certain officials at the highest levels of government, employees may **not** engage in political activity while:

- on duty;
- in a government office;
- wearing insignia identifying their office or position; or
- using a government vehicle.

Employees of the United States Secret Service are prohibited from engaging in partisan political activity.

The following categories of employees are also prohibited from engaging in partisan political activity: career members of the Senior Executive Service, Administrative Law Judges, and members of Contract Appeals Boards.

If the MSPB finds that a federal or D.C. government employee has violated the Hatch Act, what penalties may the Special Counsel request?

The Special Counsel may ask the MSPB to impose any penalty ranging from a 30-day suspension without pay to removal from federal service.

What restrictions apply to state and local government employees?

Pursuant to 5 U.S.C. § 1501, et seq., persons principally employed by state or local executive agencies in connection with programs wholly or partly financed by federal funds **may not:**

- use their official authority or influence for the purpose of interfering with or affecting the result of an election or a nomination for office;
- directly or indirectly coerce, attempt to coerce, command, or advise a state or local employee to pay, lend, or contribute anything of value to a party, committee, organization, agency, or person for political purposes; or
- be candidates for public office in partisan elections.

If the MSPB finds that a state or local government employee has violated the Hatch Act, what penalties may the Special Counsel request?

The Special Counsel may ask the MSPB to order the withholding of federal funds from a state or local agency if:

- the agency has failed to remove an employee found by the MSPB to have engaged in prohibited political activity, or
- after removal, such employee is re-employed within 18 months by a state or local agency in the

same state.

Who may file a Hatch Act complaint with the OSC?

Anyone who believes that a violation of the Hatch Act has occurred may file a complaint (see below for details). The OSC will investigate and, if warranted, prosecute the offender for violating the law.

What is the Uniform Services Employment and Reemployment Rights Act?

The Uniformed Services Employment and Reemployment Rights Act (USERRA) is the federal law that protects the employment and reemployment rights of National Guard, Armed Forces Reserve, and other uniformed service members who leave their civilian jobs to perform uniformed service. USERRA also proscribes discrimination on the basis of past, current, or future uniformed service. OSC's USERRA Unit prosecutes meritorious USERRA claims brought against federal agencies. Pursuant to a demonstration project that operates until September 30, 2007, the USERRA Unit also investigates certain federal sector USERRA cases.

How to File a Prohibited Personnel Practice, Hatch Act, or Other Complaint

Individuals may report suspected unlawful activity (including prohibited personnel practices and Hatch Act violations) to the OSC without being represented by an attorney. Complaints of such activities should be submitted to the OSC in writing. Although the use of an OSC complaint form is not required, one will be provided upon request. The form can also be found at the OSC home page on the Internet.

The following information should be included in the written submission:

- the full name and address of the person requesting OSC action, and a phone number at which the person may be contacted;
- the name and address or location of the government agency involved, including the specific office or activity that is the subject of the request for assistance;
- the job title, pay grade and employment status of the employee(s) affected by the allegedly prohibited action(s);
- an indication whether the information submitted to the OSC involves:
    - a prohibited personnel practice or other violation of civil service law, rule or regulation;
    - prohibited political activity under the Hatch Act; or
    - a violation of any other law, rule or regulation under the OSC's jurisdiction.
- a brief and accurate statement of the facts supporting the report of a prohibited activity, including:

- a concise description of the events that took place, with dates;
- the name(s) of the person(s) involved, and anyone with relevant information; and
- any pertinent documentary evidence or information currently in possession of the person requesting OSC action;

- for reports of a prohibited personnel practice:
  - a description, with date(s), of the specific personnel action(s) taken or proposed, if any;
  - a description, with date(s), of any whistleblower disclosure by the complainant: i.e., a disclosure of a violation of law, rule or regulation, gross mismanagement gross waste of funds, abuse of authority, or substantial and specific danger to public health or safety involved(limited to allegations of reprisal for whistleblower disclosures);
  - whether the complainant is covered by a collective bargaining agreement; and
- whether the matter reported has been appealed, grieved or reported under any other procedure, and if so, what action or actions have been taken.

To expedite investigations, persons filing complaints with the OSC are encouraged to respond promptly to requests for additional information. The OSC depends upon complete and accurate information to determine if a matter falls within its authority or if further action is appropriate.

All complaints and requests for appropriate forms should be directed to the OSC Officer of the Week at:

Complaints Examining Unit
U.S. Office of Special Counsel
1730 M Street, NW (Suite 218)
Washington, DC 20036-4505
Tel: (800) 872-9855 (TDD-equipped)
(202) 254-3670 (TDD-equipped)
Fax: (202) 653-0015

How to Make a Whistleblower Disclosure

Disclosures of information evidencing violations of any law, rule or regulation, gross mismanagement, gross waste of funds, abuse of authority, or a substantial and specific danger to public health or safety may be reported in confidence to:

Disclosure Unit
U.S. Office of Special Counsel
1730 M Street, NW (Suite 218)
Washington, DC 20036-4505
Tel: (800) 572-2249
(202) 254-3640
Fax: (202) 653-5151

How to Obtain a Hatch Act Advisory Opinion

Individuals may request advice about permissible and impermissible political activity under the Hatch Act, and receive an oral or written opinion, as appropriate, from the OSC. Requests may be submitted to:

Hatch Act Unit
U.S. Office of Special Counsel
1730 M Street, NW (Suite 218)
Washington, DC 20036-4505
Tel: (800) 85-HATCH [(800) 854-2824]
(202) 254-3650
Fax: 202) 653-5151
E-mail: hatchact@osc.gov

How to Report A USERRA Violation

USERRA Unit
U.S. Office of Special Counsel
1730 M Street, NW (Suite 218)
Washington, DC 20036-4505
Tel: (202) 254-3620
E-mail: userra@osc.gov

How to Obtain OSC Publications

On the Internet (at www.osc.gov):

Forms

- Complaint Form
- Whistleblower Disclosure Form
- How Your Complaint Will Be Processed By the Office of Special Counsel
- What To Expect Now That Your Complaint Has Been Referred For Further Investigation
- What To Expect Now That Your Case Has Been Referred To OSC's Prosecution Division
- Policy Statement Concerning the Disclosure of Information Regarding Personnel Practice Complaints
- Policy Statement on Disclosure and Use of Information From OSC Files

Brochures

- The Role of the U.S. Office of Special Counsel
- Employee Rights and Remedies Under 5 U.S.C., Chapters 12 and 23 (Training Guide)
- Political Activity and the Federal Employee
- Political Activity and the State and Local Employee
- Through the U.S. Government Printing Office (GPO):
- The Role of the U.S. Office of Special Counsel (GPO # 028-004-00105-9)
- Employee Rights and Remedies Under 5 U.S.C., Chapters 12 and 23 (GPO # 062-000-00050-3)
- Political Activity and the Federal Employee (GPO #062-000-00048-1)
- Political Activity and the State and Local Employee (GPO #062-000-00049-0)

OSC Online

Further information about the OSC is available on the agency's Internet home page. In addition to OSC forms and publications, the site includes a link to the OSC e-mail address for Hatch Act advisory opinions. The full address for the home page is: http://www.osc.gov .

How To Request OSC Speakers

Requests for OSC speakers at training sessions, conferences and similar events should be sent to:

Outreach Specialist
U.S. Office of Special Counsel
1730 M Street, NW (Suite 218)
Washington, DC 20036-4505
Tel: (202) 254-3600
Fax: (202) 254-3711

OSC Phone Numbers to Note

Complaints Examining Unit (CEU): (TDD-equipped)	(202) 254-3670
CEU (Toll-Free): (TDD-equipped)	(800) 872-9855
Hatch Act (HA) Unit:	(202) 254-3650
HA (Toll-Free):	(800) 85-HATCH (800) 854-2824
Disclosure Hotline (DH):	(202) 254-3640
DH (Toll-Free):	(800) 572-2249
USERRA Unit:	(202) 254-3620

OSC Field Offices

Dallas Field Office
525 Griffin Street, Room 824, Box # 103
Dallas, TX 75202
(214) 747-1519

San Francisco Bay Area Field Office
1301 Clay Street (Suite 365S)
Oakland, CA 94612-5217
(510) 637-3460

Midwest Field Office
211 West Fort Street (Suite 521)
Detroit, MI 48226
(313) 226-4441
(313) 226-5606

Questions about OSC?

Call Customer Service Unit (CSU): (202) 254-3600

(The preceding information is provided to the public as a general guide. It is not intended to create any rights, benefits or privileges, and should not be considered a regulatory or other legal authority.)

RIF

OSC Publication: Your Rights as a Federal Employee

YOUR RIGHTS AS A FEDERAL EMPLOYEE

ENFORCED BY

THE U.S. OFFICE OF SPECIAL COUNSEL

1. THE U.S. OFFICE OF SPECIAL COUNSEL (OSC) is an independent agency that investigates and prosecutes allegations of prohibited personnel practices (PPP).

WHAT IS A PROHIBITED PERSONNEL PRACTICE (PPP)?:

Under 5 U.S.C. §2302(b)(1)-(b)(13) a federal employee authorized to take, direct others to take, recommend or approve any personnel action may not:

- **Discriminate (including discrimination based on marital status and political affiliation).** *EXAMPLE: Supervisor Joe refuses to promote Employee Jane because Jane is a registered Republican; or his refusal is because she is a single mother. (OSC will generally defer Title VII discrimination allegations to the EEO process, rather than duplicating already existing procedures.)*
- **Solicit or consider employment recommendations based on factors other than personal knowledge or records of job-related abilities or characteristics.** *EXAMPLE: Selecting Official Joe hires Applicant Jack based on Senator Smith's recommendation that Jack be hired because Jack is a constituent, or fails to hire Applicant Jane because of Congressman Smith's recommendation based on the Congressman's friendship with Jane's parents.*
- **Coerce the political activity of any person, or take action against any employee as reprisal for refusing to engage in political activity.** *EXAMPLE: Supervisor Jane takes away significant job duties of Employee Jack because Jack will not make a contribution to Jane's favorite candidate.*
- **Deceive or willfully obstruct any person from competing for employment.** *EXAMPLE: Supervisor Joe, located in Headquarters, orders that no vacancy announcements be posted in the field office where Employee Jack works because he does not want Jack to get a new job; or falsely states that there will be extensive travel in the position when he knows that there is no travel.*
- **Engage in nepotism.** *EXAMPLE: Second-level Supervisor Jane asks First-level Supervisor Joe to hire her son; or to promote her daughter.*
- **Take a personnel action against an employee because of whistleblowing.** *EXAMPLE: Supervisor Joe directs the geographic reassignment of Employee Jack because Jack reported safety violations to the agency's Inspector General; or because employee Jill reported a gross waste of funds to the Office of Internal Affairs.*
- **Take a personnel action against any employee because of the exercise of an appeal, complaint, or grievance right.** *EXAMPLE: Supervisor Jane places Employee Jack on an undesirable detail because Employee Jack filed an administrative grievance about his performance rating.*
- **Discriminate against an employee on the basis of conduct, which does not adversely affect the performance of the employee, including discrimination based on sexual orientation.** *EXAMPLE: Jack's employment is terminated because he attended a "Gay Pride" march, or he attended a "Pro-Life" event; or he attended an animal rights rally; or he attended a gun-owners' rights meeting.*
- **Take or fail to take a personnel action, if such action would violate a veterans' preference requirement.** *Example: Supervisor Jane hired Employee Jack, without considering Veteran Jennifer, who was included on the list of eligible employees. (OSC's jurisdiction is for disciplinary actions only; the Dept. of Labor has jurisdiction to investigate for corrective actions.).*

RIF

OSC Publication: Your Rights as a Federal Employee (continued)

- **Influence any person to withdraw from competition for a position to improve or injure the employment prospects of any other person.** *EXAMPLE: Supervisor Jane, in an effort to hire Employee Joe, tells Employee Jack that he should not apply for a position because he is not qualified and will never be selected. Employee Jack is qualified.*
- **Give an unauthorized preference to a person to improve or injure the employment prospects of any particular employee or applicant.** *EXAMPLE: Supervisor Jane specifies that Spanish-speaking skills are necessary for a vacant position, for the purpose of selecting Employee Jack, who speaks fluent Spanish. The position, however, does not require Spanish-speaking skills.*
- **Take a personnel action against an employee which violates a law, rule, or regulation which implements a merit systems principle.** *EXAMPLE: Supervisor Joe terminates the probationary appointment of Employee Jack because of Jack's letter to the editor criticizing affirmative action - a valid exercise of First amendment rights, a law implementing a merit system principle.*
- **Implement or enforce a nondisclosure agreement or policy lacking notification of whistleblower rights.** *EXAMPLE: A manager requires all employees in his program to sign a non-disclosure agreement that prohibits the employees from discussing the program in any way and fails to notify employees of protected channels for making disclosures.*

What can you do if you believe a PPP has been committed?

An employee who believes a PPP has been committed can file a written complaint with the U.S. Office of Special Counsel. Complaint forms are available on the Web at www.osc.gov. Employees do not need attorneys to file a complaint. OSC is an independent and prosecutorial agency. It will investigate allegations of prohibited personnel practices, and seek any corrective and disciplinary action.

II. The U.S. Office of Special Counsel also receives confidential disclosures and enforces the Hatch Act

RECEIVING CONFIDENTIAL DISCLOSURES (5 U.S.C. §1213):
Current and former federal employees and applicants can confidentially report information evidencing a violation of any law, rule, or regulation, gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. The OSC has the authority to require the head of the agency concerned to investigate the matter if OSC determines that a disclosure has been made.

ENFORCING THE HATCH ACT (5 U.S.C. §7321-26):
The Office of Special Counsel is authorized to issue advisory opinions that respond to federal employee questions about whether or not they may engage in specific political activities under the Act. The OSC also prosecutes violations of the Hatch Act before the Merit Systems Protection Board. These violations include: using official authority to interfere with an election result, soliciting, accepting or receiving political contributions; soliciting or discouraging political activity of persons before the employing agency; and running for public office in a partisan political election.

Need additional information?

- Information on filing a complaint: 202-254-3600 or 800-872-9855.
- Information on making a disclosure: 202-254-3640 or 800-572-2249.
- Updated and detailed information on OSC and its procedures- visit our web page: www.osc.gov.

U.S. Office of Special Counsel
1730 M Street N.W., Suite 218
Washington D.C. 20036-4505

RIF

OSC Publication: Know Your Rights When Reporting Wrongs

U.S. Office of Special Counsel

Know Your Rights When Reporting Wrongs

Whistleblower disclosures can save lives as well as billions of taxpayer dollars. They play a critical role in keeping our government honest, efficient and accountable. Recognizing that whistleblowers root out waste, fraud and abuse, and protect public health and safety, federal laws strongly encourage employees to disclose wrongdoing. Federal laws also protect whistleblowers from retaliation.

The U.S. Office of Special Counsel (OSC) plays an important role in helping whistleblowers. OSC is an independent agency. OSC protects federal employees from "prohibited personnel practices," including whistleblower retaliation and unlawful hiring practices, such as nepotism. OSC also provides an independent, secure channel for disclosing and resolving wrongdoing in federal agencies. This guide provides a summary of whistleblower protections and avenues available to employees to disclose wrongdoing. For more information, please visit OSC's website at www.osc.gov.

Where can I report wrongdoing?

Federal employees have many options to disclose wrongdoing. They can:

- tell a supervisor or someone higher up in management;
- report the issue to their agency's Office of Inspector General (OIG); or
- file a complaint with OSC.

Current and former federal employees and applicants can confidentially report information to an OIG or OSC about any of the following types of wrongdoing:

- a violation of any law, rule, or regulation,
- mismanagement,
- a gross waste of funds,
- an abuse of authority, or
- a substantial and specific danger to public health or safety.

OSC protects federal employees who make disclosures to OSC or an OIG from retaliation.

Can I keep my identity confidential?

Yes. Most Inspectors General have hotlines that allow employees to make confidential disclosures. Inspectors General are prohibited from disclosing an employee's identity unless the IG determines that disclosure is unavoidable or is compelled by a court order.

If you file a disclosure with OSC, your identity will not be shared outside of OSC without your consent. OSC may disclose your identity only if OSC determines that it is necessary because of an imminent danger

OSC Publication: Know Your Rights When Reporting Wrongs (cont.)

to public health or safety or an imminent violation of any criminal law.

What will OSC do once I make a disclosure?

When a federal employee discloses wrongdoing, OSC evaluates the information and interviews the federal employee. OSC determines whether it is substantially likely that the employee's allegation – or any portion of it – can be proven and whether it discloses a violation of a law, rule, or regulation; gross mismanagement; a gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety.

If it meets that standard, OSC will require the agency to investigate and submit a report of the agency's findings to OSC. The whistleblower then has an opportunity to comment on the agency report. Those comments, together with any comments or recommendations by the Special Counsel, are sent with the agency report to the President and congressional oversight committees. The agency report is usually made available to the public.

Are whistleblowers protected from retaliation?

Yes. The Whistleblower Protection Act prohibits retaliation. This means it is unlawful for agencies to take or threaten to take a personnel action against an employee because he or she disclosed wrongdoing. Personnel actions can include poor performance review, demotion, suspension or termination. In addition, the law prohibits retaliation for filing an appeal, complaint, or grievance; helping someone else file or testifying on their behalf; cooperating with or disclosing information to the Special Counsel or an Inspector General; or refusing to obey an unlawful order.

However, disclosures of information specifically prohibited by law or required by Executive order to be kept secret are protected only when made to an OIG or OSC.

Are disclosures to Congress protected?

Yes. Federal law establishes that a federal employee has the right to communicate with and provide information to the United States Congress.

What can you do if you believe whistleblower retaliation occurred?

If you believe that an agency has retaliated against you because of your whistleblowing, you can:

- file a complaint with OSC, which may seek corrective action when warranted;
- file a union grievance; or
- if you have been subject to a significant personnel action, you can file an appeal with the Merit Systems Protection Board (www.mspb.gov) and assert whistleblower retaliation as a defense.

Note that an employee may choose only one of these three options when appealing a significant personnel action.

OSC Publication: Know Your Rights When Reporting Wrongs (cont.)

What relief is available to an employee who has suffered retaliation for whistleblowing?

Many forms of relief are available. They include job restoration, reversal of suspensions and other adverse actions, back pay, reasonable and foreseeable consequential damages, such as medical costs, attorney fees, and compensatory damages. In addition, damages may be awarded for attorney fees and expenses incurred due to retaliation.

Can the OSC delay a personnel action while the matter is investigated?

Yes. An individual may ask OSC to delay, or "stay," an adverse personnel action pending an investigation. OSC will consider requesting a delay of a personnel action if OSC has reasonable grounds to believe that a prohibited personnel action was taken.

How can the OSC remedy a prohibited personnel practice?

Current and former federal employees and applicants for federal employment may report suspected prohibited personnel practices to OSC. Their complaint will be investigated. If there is sufficient evidence to prove a violation, OSC can seek corrective action, disciplinary action, or both. Alternatively, parties in selected cases may agree to mediate their dispute in order to reach a mutually agreeable resolution of the complaint.

OSC may attempt to resolve a case with an agency at any stage. If an agency refuses to provide corrective action, then OSC can take the case to the MSPB. The MSPB can order the agency to take corrective action. Such litigation begins with the filing of a petition by OSC, alleging that there are reasonable grounds to believe that a prohibited personnel practice occurred, is occurring, or is about to occur.

Can a manager be held accountable for retaliating against a whistleblower?

Yes. OSC may seek disciplinary action against any employee who commits a prohibited personnel practice. If an agency fails to take disciplinary action, then OSC can bring a disciplinary action case to the MSPB against the employee who committed the prohibited personnel practice. If the MSPB finds that an individual has committed a prohibited personnel practice, it can order disciplinary action, including removal, reduction in grade, debarment from federal employment for up to five years, suspension, reprimand, or a fine of up to $1,000.

1730 M Street NW
Suite 218
Washington, DC 20036
Phone: 202-254-3600
Fax: 202-254-3711
www.osc.gov

POLITICAL ACTIVITY

General

Federal employees, along with all Americans, have the privilege and obligation of deciding political contests at the polls. Unlike other Americans, however, civil servants are restricted in the nature and extent of their political activities by the Hatch Act, a law passed in 1939 in an effort to protect the Civil Service from the abuses of the "Spoils System." The Hatch Act applies to all Secret Service employees, including those in the Senior Executive Service, whether on or off duty or on leave. This section describes some permitted and prohibited political activities under the Hatch Act.

The Hatch Act was amended on February 03, 1994, which expanded political activities permitted for Federal employees. However, Secret Service employees are excluded in the amendment and continue to be covered under the old law.

If uncertain about a particular political activity, employees should contact the Office of the Chief Counsel for guidance **prior** to engaging in the activity. Severe penalties are prescribed for Hatch Act violations.

Permitted Activities

All employees are free to engage in political activity to the widest extent consistent with the restrictions imposed by the law. Employees may:

1. Register and vote in any election.

2. Express political opinions privately and publicly as long as he or she does not take an active part in partisan political management or campaigns.

3. Wear a political badge or button or display a political sticker on a private automobile, subject to work-related limitations.

4. Make a voluntary campaign contribution to a political party or organization.

5. Accept appointment to public office, such as membership on boards of education and school committees (but not to interfere or conflict with Federal employment).

6. Participate in or be a candidate for office in nonpartisan elections, and hold such office (but not to interfere or conflict with Federal employment).

7. Serve in a position which performs nonpartisan duties as prescribed by State or local law, such as an election judge or clerk.

8. Be politically active in connection with an issue not specifically identified with a political party, such as a

constitutional amendment, referendum, or similar issue.

9. Participate in the nonpartisan activities of a civic, community, social, labor, professional, or similar organization.

10. Be a member of a political party or other political organization and attend meetings and vote on issues, but not take an active part in managing the organization.

11. Attend a political convention, rally, fund-raising function, or other political gathering, but not take an active part in conducting or managing such gathering.

12. Sign petitions, including nominating petitions, but not initiate them or canvass for signature if they are nominating petitions for candidates in partisan elections.

13. Petition Congress or any Member of Congress, such as by writing to Representatives and Senators to express opinions on particular issues.

Prohibited Activities

The general prohibitions on employees are that they may not use their official authority or influence to interfere with or affect the result of an election, and that they may not take an active part in partisan political management, or in partisan political campaigns. Employees may not:

1. Be a candidate for nomination or election to a national or state office.

2. Become a partisan candidate for nomination or election to public office.

3. Campaign for or against a political party or candidate in a partisan election for public office or political party office.

4. Serve as an officer of a political party, a member of a National, State or local committee of a political party, an officer or member of a committee of a partisan political club, or be a candidate for any of these positions.

5. Participate in the organizing or reorganizing of a political party, organization, or club.

6. Solicit, receive, collect, handle, disburse, or account for assessments, contributions, or other funds for a partisan political purpose or in connection with a partisan election.

7. Solicit political contributions from other Federal employees; solicit or receive political contributions in buildings where Federal employees work.

8. Make political contributions to other Federal employees.

9. Sell tickets for or otherwise actively promote such activities as political dinners.

10. Take an active part in managing the political campaign of a candidate in a partisan election for public office or political party office.

11. Work at the polls on behalf of a partisan candidate or political party by acting as a checker, challenger, or watcher, or in a similar partisan position.

12. Distribute campaign material.

13. Serve as a delegate, alternate, or proxy to a political party convention.

14. Address a convention, rally, caucus, or similar gathering of a political party in support of or in opposition to a candidate for public office or political party office, or on a partisan political question.

15. Endorse or oppose a candidate in a partisan election through a political advertisement, broadcast, campaign literature, or similar material.

16. Use his or her automobile to drive voters to the polls on behalf of a political party or candidate in a partisan election.

PUBLIC RELATIONS GUIDELINES

Media Policy

All media inquiries and requests for interviews, without exception, must be referred to the appropriate SAIC or Division Chief. However, inquiries of national significance or from national media entities must be forwarded to the Office of Government and Public Affairs (GPA), Public Affairs Program (PAF).

Only field office SAICs or their designee(s) are authorized to deal with their local media on matters pertaining to local issues. SAICs are permitted to designate another supervisor or agent to act as an official spokesperson for that district in dealing with the local media. In cases where the SAIC has designated a spokesperson, the Assistant Director, GPA, is to be provided the name(s) via memorandum. With their SAIC's approval, RAICs are permitted to interact with the local media on local issues. SAICs are strongly encouraged to coordinate with PAF when dealing with the press.

SAICs and RAICs may answer general questions from the media about presidential visits, e.g., by describing routine Secret Service preparations for any protectee visit, including information found on the Secret Service external Web site and in the pamphlet, "The Secret Service Story," published by GPA. SAICs should never comment on protective means or methods, travel plans, itinerary, hotel information, motorcade routes, or any other details surrounding a particular visit, even when this information has been publicized.

It is imperative that Secret Service supervisors refrain from confirming upcoming presidential and vice presidential visits prior to the White House's formal announcement of such visits. Always refer such questions to the White House Press Office at 202-456-2580 or to the protectee's staff office. Supervisors should encourage local law enforcement counterparts to refrain from commenting on protective visits until the respective trip has been announced by the White House.

Headquarters SAICs/Division Chiefs, including protective detail SAICs, should not respond to media inquiries without first consulting with PAF. Under no circumstances shall SAICs or RAICs comment on Secret Service issues of national significance. Under no circumstances should any non-designated employee comment to any member of the media, whether local or national, without the prior approval of their SAIC/Division Chief or the SAIC, PAF.

SAICs are required to make timely notifications of events that may generate either national media or congressional inquiries. PAF will prepare any required official responses. Notifications can be made to GPA on a 24-hour basis by calling 202-406-5708.

SAICs and their designee(s) are encouraged to use television, radio, print media and personal appearances to inform the public of the Secret Service's dual mission and responsibilities. When responding to the media, credit to other law enforcement agencies and the local U.S. Attorney's offices should be given, when appropriate.

It should be noted that the release of information, coordinated with the appropriate Federal/State prosecutor's office relating to criminal and civil proceedings, is guided by Title 28, Code of Federal Regulations, section 50.2. More specific guidelines are enumerated in the following sections.

Notifications

National Issues and Headquarters Interest

Arrests or incidents of a protective or investigative nature that could lead to nationwide publicity, or that could prompt media inquiries at Headquarters, should be relayed to the SAIC, PAF immediately. Examples include shooting incidents, arrests of well-known individuals, unusually large counterfeit seizures, aggravated protective intelligence arrests, and incidents occurring during protectee visits. Incidents involving Secret Service personnel that could generate unusual media interest should be reported immediately. At the time of the notification of the incident, the SAIC, RAIC, and PAF staff will coordinate the release of information. No information should be released until the Assistant Director, GPA, or designee, has been notified and has approved the release of information.

When more than one district is involved in the arrest or incident, or if the released information will affect another district, all releases to the media should be coordinated with the appropriate districts, as well as with PAF.

Local Press Releases and Press Announcements

Press releases issued by a local field office, U.S. Attorney's Office, or local prosecutor's office, should be sent in advance to PAF for review and potential inclusion in the daily news clips and/or the Public Affairs Web page.

Authorized Releases

Releasing Information Concerning Protective Intelligence Cases

In compliance with Pub. L. 93-579, The Privacy Act of 1974, as amended, it is Secret Service policy to not discuss threat cases if no arrest or formal judicial proceeding has occurred.

Protective intelligence cases that could generate media interest should be reported to the SAIC, PAF as soon as possible. The SAIC, PAF, will respond to media inquiries after discussions with the Assistant Director, Office of Protective Research.

In response to local media inquiries about protective intelligence arrests or those involving formal judicial proceedings, SAICs or their designated spokesperson should release only the following information:

- The defendant's name, age, city of residence, and sex.
- The nature of the charge or code violation.

SAICs or their designated spokesperson should not release information concerning the specific nature of the threat involved.

In instances where charges have been filed, the media may obtain copies of the criminal complaint and supporting affidavit from the prosecuting U.S. Attorney or local prosecutor's office. These documents contain specific information relating to the investigation. SAICs and RAICs should **not** release copies of these legal documents to the media. When the media has obtained the criminal complaint and affidavit in a protective intelligence investigation, SAICs and RAICs should not comment further on the information.

SAICs and RAICs must use caution and be aware of the possible adverse effects of publicity on the Secret Service's protective mission. With regard to threat cases, Section 9-65.140 of the U.S. Attorney's Manual requests that U.S. Attorneys carefully consider the possible adverse effects caused by media attention before releasing information to the public about threats against Secret Service protectees.

Refer to the Protective Research Manual, section INT-03, Relationship to Other Federal Agencies, for a further explanation of the adverse effects of publicity in such cases.

Releasing Information about Criminal Non-Protective Intelligence Cases

These guidelines apply from the time a person is the subject of a criminal investigation to the time any judicial proceeding resulting from the investigation has terminated.

SAICs or their designated spokesperson should coordinate the release of any information on a criminal case with the local U.S. Attorney and/or local prosecutors.

If more than one district is involved in the investigation, or if the released information will affect another district, all releases to the media should be coordinated with each district and GPA. Following an arrest, an authorized Secret Service spokesperson may make public the following information, subject to specific limitations imposed by law, court rule or order:

- The defendant's name, sex, age, city of residence.
- The substance or text of the charge such as in a complaint, indictment or information.
- The identity of the investigating and arresting agency(ies) and the length or scope of the investigation.
- The circumstances immediately surrounding the arrest, including time and place, resistance, pursuit, possession and use of weapons, and physical items seized at the time of arrest.

Disclosures should include only factual matters and should not include subjective observations. Because of the danger of judicial prejudice, avoid disclosures immediately before and during trial. Any statement or release should be made only when circumstances absolutely demand a disclosure of information and should include only information that, clearly, is not prejudicial. The release of certain types of information generally tends to create the danger of prejudice. Premature release of information might seriously interfere with the success of an investigation and judicial handling of a case.

Therefore, SAICs and RAICs **must not:**

- Comment on pending investigations or the names of persons involved in pending investigations.
- Make statements revealing investigative techniques used in any case, pending or closed.
- Make reference to investigative procedures such as handwriting examination, fingerprints, polygraph examinations, ballistic tests, laboratory tests, or the refusal by the defendant to submit to such tests or examinations.
- Comment on statements, admissions, confessions or alibis attributable to a defendant, or the refusal or failure of the accused to make a statement.

- Make observations about a defendant's character.
- Release information concerning a defendant's prior criminal record.
- Make statements concerning the identity, testimony or credibility of witnesses.
- Make statements concerning evidence or argument in a case, whether or not it is anticipated that such evidence or argument will be used at trial.
- Express any opinion as to the defendant's guilt, the possibility of a guilty plea to the offense charged or the possibility of a plea to a lesser offense.
- Furnish any statement or information that may be reasonably expected to influence the outcome of a defendant's trial.
- Take action to encourage or help the media photograph or televise a defendant or accused person being transported or held in Federal custody.
- Make available photographs of a defendant, unless releasing the photograph serves a law enforcement function.

In instances where charges have been filed, the media may obtain copies of the criminal complaint and supporting affidavit from the prosecuting U.S. Attorney or local prosecutor's office. These documents will contain specific information relating to the investigation and subsequent arrest. SAICs and RAICs should **not** release copies of these legal documents to the media. When the media has obtained the criminal complaint and affidavit in a criminal investigation that does not involve protective intelligence issues, SAICs and RAICs should limit their responses to that information contained in those documents. SAICs and RAICs should coordinate with the U.S. Attorney's Office and/or local prosecutors to avoid any potential compromise to pending judicial proceedings.

This statement of policy is not intended to restrict the release of information about a defendant who is a fugitive from justice, but rather to set forth general guidelines. There may be times when releasing additional information will further the fair administration of justice and the law enforcement process. Secret Service representatives who wish to release information beyond these policy guidelines must request approval from the Assistant Director, GPA.

Restricted Information

Certain information should never be released. Providing premature publicity to criminal actions may hinder investigative efforts. SAICs and RAICs **must not**:

- Give publicity to new counterfeit notes until, at the SAIC's and RAIC's discretion, a sufficient quantity has been circulated for a reasonable period of time. Public warning may hinder efforts to arrest passers and manufacturers. Refer to the Investigative Manual, section CID-24, Counterfeit Warning Notices, for guidance on appropriate restrictions on the release of such information.
- Express opinion publicly or speculate about sources of counterfeit notes or any contraband.
- Exaggerate facts or statistics. Newspaper headlines that declare "millions of dollars" in counterfeit notes are circulating serve only to alarm the public. The objective of alerting money handlers can be achieved through accurate reports.
- Disclose for publication the name of any undercover agent or the office to which the agent is assigned.
- Confirm the utilization of confidential informants or reveal their identities.
- Give a media representative advance notice of a contemplated arrest or seizure, or permit the representative to accompany them on official investigations, unless approval from both the AD - Investigations and the AD - GPA has been obtained.
- Release information about protectees' itineraries, motorcade routes or other specific information surrounding scheduled or potential visits, even when this information has been publicized by some other source.

- Make remarks relating to the private lives of protectees, their families or staffs, or discuss nonpublic events or information pertaining to these individuals, except for information released by the AD-GPA.
- Make remarks concerning specific matters relating to both criminal and protective responsibilities that deal with the Secret Service's means and methods of operation, staffing, procedures or techniques of operation.
- Furnish media representatives with materials from official files.
- Release loss information as it relates to a specific credit card company (e.g., Master Card, Visa, American Express, and other card issuers) without the consent of the company. Industry-wide loss figures for dissemination to the public and the media are available from the Criminal Investigative Division.

Approval of Material for External Publication or Presentation

Employees, offices, divisions, and branches preparing written, electronic, or audio/visual materials for external publication or dissemination outside the Secret Service must coordinate with GPA. (This does not include documents routinely produced as part of USSS security planning activities and distributed to appropriate law enforcement entities.) This office will review the material, forward it to the Chief Counsel, and, when circumstances warrant, to the Information Quality Officer, Management and Organization Division (MNO) for review; resolve any procedural or regulatory difficulties; and return it to the requesting office or the Visual Information Branch (VIB) of the Forensic Services Division for processing. Employees seeking to publish articles outside of their position at the Secret Service must individually request permission to engage in outside employment and address all the components of such a request as outlined in the Human Resources and Training Manual, section PER-05(02), Employee Responsibilities and Conduct.

Approval of Material to be Posted on the Internet

The Internet is a powerful and effective tool to effectively communicate general interest material to the public. However, all such material must be reviewed both for operational security considerations and for conformance with official Secret Service policy and procedures. To ensure that such reviews are accomplished, all offices and divisions posting material to the Secret Service's Internet page must obtain the approval of the Office of Government and Public Affairs. PAF will review all material and coordinate with the Director's executive staff as required. No material is authorized for posting to the Secret Service's external Internet site until approval is granted by the SAIC, PAF.

UNITED STATES SECRET SERVICE TABLE OF PENALTIES

Introduction

The United States Secret Service's (Secret Service) Table of Penalties is intended to serve as a **guide** in determining appropriate corrective, disciplinary, or adverse actions for common offenses and supersedes all previous policies and practices regarding disciplinary offenses and penalties.

The Offense Codes outlined in the Table of Penalties do not cover every possible offense but rather provide a general description of certain types of misconduct, whether committed on or off-duty, for which employees may be disciplined. The absence of a specific Offense Code covering an act does not mean that such an act is condoned, permissible, or would not result in disciplinary or adverse action. Offenses not described in the Offense Codes may be separately identified and result in appropriate disciplinary or adverse action, provided there is a nexus between the misconduct and the efficiency of the service. Employees are encouraged and expected to report through their chain of command, or the Inspection Division Hotline, or the DHS Office of the Inspector General hotline, information that indicates another employee may have engaged in misconduct described in the Table of Penalties. Supervisors are required to report through their chain of command an employee's misconduct involving violations set forth in the Table of Penalties. Failure of a supervisor to report information required by this policy may result in disciplinary action. See Offense Code 5.6A.

Purpose and Progressive Nature of Discipline

The Secret Service is a world renowned, pre-eminent law enforcement agency and is distinguished by its responsibilities to protect the president, vice-president, and other national leaders, visiting world leaders, and designated National Special Security Events. As such, the Secret Service employs advanced recruitment strategies designed to attract and retain employees who possess the highest levels of aptitude and integrity. All Secret Service employees are held to a high standard of conduct and expected to be worthy of trust and confidence. The Secret Service's disciplinary and adverse action processes serve to ensure adherence to the highest standards of conduct. Disciplinary measures are imposed to promote behaviors and principles that champion the pursuit of organizational achievement and excellence. The discipline model of the Secret Service is designed to incentivize self-discipline at all levels. Discipline at the Secret Service is progressive in nature, meaning that subsequent acts of misconduct are treated with increasing severity, especially but not exclusively, when the acts of misconduct are similar in nature and/or the passage of time between occurrences is of significant relevance. Certain offenses are so egregious that a single act is sufficient to warrant an employee's removal from employment with the Secret Service.

Penalty Ranges and Factors Considered in Determining the Penalty

The Secret Service's Penalty Guidelines are expressed in terms of a Standard Penalty, a Mitigated Range, and an Aggravated Range. Selection of an appropriate penalty involves a responsible balancing of the relevant factors in each case. The aggravating and mitigating factors listed in the Penalty Guidelines are a general description of certain factors that will result in higher or lower penalties depending on the specific case's circumstances. The factors listed in the Penalty Guidelines are illustrative and not exhaustive.

In addition, the Douglas Factors set forth below will be considered in every case prior to determining the penalty. Not all of these factors are applicable to every case, and the deciding official will balance the relevant ones.

The Douglas Factors are:

1) The nature and seriousness of the offense, and its relation to the employee's duties, position, and responsibilities, including whether the offense was intentional, technical, or inadvertent; or was committed maliciously or for gain, or was frequently repeated;

2) The employee's job level and type of employment, including supervisory or fiduciary role, contacts with the public, and prominence of the position;

3) The employee's past disciplinary record;

4) The employee's past work record, including length of service, performance on the job, ability to get along with fellow workers, and dependability;

5) The effect of the offense upon the employee's ability to perform at a satisfactory level and its effect upon supervisors' confidence in the employee's ability to perform assigned duties;

6) Consistency of the penalty with those imposed upon other employees for the same or similar offenses;

7) Consistency of the penalty with any applicable agency table of penalties;

8) The notoriety of the offense or its impact upon the reputation of the agency;

9) The clarity with which the employee was notified about any rules that were violated in committing the offense, or had been warned about the conduct in question;

10) The potential for the employee's rehabilitation;

11) Mitigating circumstances surrounding the offense such as unusual job tensions, personality problems, mental impairment, harassment; or bad faith, malice or provocation on the part of others involved in the matter; and

12) The adequacy and effectiveness of alternative sanctions to deter such conduct in the future by the employee or others.

The penalty for misconduct will be mitigated or aggravated only after full and fair consideration of all available information. The Table of Penalties is a guide to help ensure consistent application of similar

penalties for similar offenses, but the selection of a penalty should always be appropriate to the facts of the case.

Statutory, regulatory, or policy citations listed in the Offense Codes or Penalty Guidelines are provided strictly for the convenience of the user. A specific reference to a statute, regulation, or policy in the Offense Codes or Penalty Guidelines does not mean that the citation is the only one applicable or that a citation is required to determine a violation. Although a criminal statute or conduct may be cited, the level of proof required for disciplinary purposes does not rise to the level required for criminal prosecution.

Suspensions are imposed in calendar days, not work days, and the days are intended to be served concurrently. Demotions may also be considered as an appropriate disciplinary measure even though they are not specifically designated as a penalty in the Penalty Guidelines. (Consult with designated Secret Service Office of Integrity officials for additional guidance.)

Combination of Penalties

In cases where more than one offense is substantiated against an employee, the penalties may be added together. However, in proposing a disciplinary action, the proposing official will not assess multiple penalties where the substantiated charges are essentially restatements of the same misconduct. Further, if an employee commits more than one kind of offense, then the employee may be subject to a higher penalty to include removal, even when one offense, standing alone, would not necessarily result in the higher penalty or removal.

Nexus

The listed offenses apply to all Secret Service personnel regardless of position or title. Law enforcement officials and supervisory personnel may be held to a higher standard of conduct than other employees. The term "on duty" refers to the period when an employee is performing an official duty or acting in an official capacity, whether or not the employee is being paid at the time (e.g., misconduct occurring while an employee is driving an official Government Owned Vehicle (GOV) at the end of the employee's work day, traveling on a commercial carrier while armed, and/or is on official travel, is considered "on duty" for administrative disciplinary purposes).

An employee may be disciplined for misconduct that occurs off duty. In such circumstances, there must be a nexus between the employee's misconduct and the efficiency of the Secret Service. A nexus may be established by the effect of the misconduct on the mission of the Secret Service, publicity or notoriety arising from the misconduct, the misconduct's effect on the Secret Service's ability to rely on the integrity, honesty, or judgment of the employee, and other similar and relevant factors.

Senior Executive Service (SES)

Title 5 of the Code of Federal Regulations, section 752.601 provides that members of the SES may not receive an adverse action of less than 15 days. Accordingly, where the Penalty Guidelines indicate a suspension of one to 14 days for an offense, that sanction cannot be imposed on an SES employee. When the proposing and deciding officials conclude that an adverse action of more than a three-day suspension, but less than a 15-day suspension is appropriate, an SES employee will generally receive a minimum of a 15-day suspension. When the proposing and deciding officials conclude that an adverse action of a one-day to a three-day suspension is appropriate, an SES employee may receive a letter of reprimand rather than a minimum of a 15-day suspension if, after weighing the heightened behavioral and managerial expectations associated with SES personnel against the facts and circumstances of the case, the deciding official determines that a 15-day suspension is not appropriate.

Exceptions to the Offense Codes and Penalty Guidelines

The security clearance process is separate from the disciplinary process and this guidance does not apply to security clearance determinations regarding the denial, suspension, or revocation of eligibility for access to classified information. However, as outlined in the Offense Codes, when an employee's Top Secret security clearance has been suspended or revoked, a proposed indefinite suspension may be issued; and when an employee's Top Secret security clearance has been finally revoked by the Security Appeals Board, a proposal to remove the employee from Federal service will be issued. Consistent with this guidance, an employee may be subject to disciplinary or adverse action for misconduct that raises security concerns regardless of whether or not the Security Management Division (or successor division) takes a security related action in the matter.

The Medical Review Board process is also separate from the disciplinary process, and this guidance does not apply to removals proposed by the Medical Review Board based on inability to perform the essential functions of an employee's position due to his or her medical condition.

This guidance also does not apply to performance deficiencies which may be addressed through the use of performance improvement plans (see PER-06(03) or its successor HUM section), to denials of within-grade increases (see PER-06(04) or its successor HUM section), or to removal or demotion actions taken under title 5 of the United States Code, chapter 43.

In addition, a matter may be referred to other Secret Service divisions for appropriate action regardless of whether or not disciplinary action is taken. For example, a matter may be referred to the Financial Management Division for the recoupment of monies owed to the government; to the Safety, Health and Environmental Programs Division for a fitness-for-duty or medical examination; and to the Security Management Division for review.

Although some offenses may fall within an Offense Code listed in the Table of Penalties, supervisors may consider issuing informal discipline to an employee in certain situations. Informal discipline includes either a verbal counseling or a memorandum of counseling. A verbal counseling informs the employee of his/her action that constitutes misconduct, illustrates the negative effects of such conduct, explains to the employee what should have been done, and warns the employee of possible further disciplinary action if the violation reoccurs. Managers and supervisors may verbally counsel employees without prior consultation with ITG for those matters listed below. A memorandum of counseling states specifically what occurred, what policy

or regulation was violated, what the employee should have done, and is issued to the employee in writing by his/her supervisor (following consultation with ITG). See ITG-06(02) for specific information.

Supervisors and managers have the responsibility of using good judgment when considering whether informal discipline may be appropriate, based on the totality of the circumstances. In the following instances, a supervisor or manager may issue informal discipline:

- Tardiness – non-habitual violations
- Absent without leave – less than one workday
- Appearance policy – minor violations
- Performance – minor issues that do not affect the mission
- Discourtesy or disruptive behavior– minor, non-habitual violations
- Failure to follow instructions – minor, non-habitual violations
- Failure to follow leave policies – minor, non-habitual violations
- Loss of Government property valued at $500 or less (non-protective equipment or weapons)
- Loss of Government-issued identification or access cards (does not include badges)
- Security violation (first offense)

For minor offenses other than those specifically listed above, supervisors and managers must address the matter as indicated below:

If a Letter of Reprimand is included within the penalty range, supervisors must: 1) report, through their chain of command, an employee's misconduct to the Intake Group; or, alternatively, 2) notify their chain of command of the potential for informal discipline and, with agreement of the Directorate, contact the Deputy Chief Integrity Officer for approval to address the matter through informal discipline. The supervisor must inform the employee if the matter is being referred to the Intake Group (unless the matter involves an OIG or ongoing investigation, in which case the supervisor should contact the Inspection Division prior to notifying the employee to ensure notification is appropriate at that time).

If a Letter of Reprimand is not included within the penalty range for an offense, supervisors must report, through their chain of command, an employee's misconduct to the Intake Group. The supervisor must also inform the employee that the matter is being referred to the Intake Group (unless the matter involves an OIG or ongoing investigation, in which case the supervisor should contact the Inspection Division prior to notifying the employee to ensure notification is appropriate at that time).

For information concerning the Intake Group, see ITG-06(01).

Appendix A:
United States Secret Service Table of Penalties
(Offense Codes – Applicable to Secret Service's Internal Disciplinary Process)

Offense Codes – Applicable to Secret Service's Internal Disciplinary Process
• The Offense Codes are arranged by category of offenses. Within each category, the offenses are arranged alphabetically. • Unless otherwise noted, the listed offenses apply to all Secret Service personnel, regardless of position or title. • The term "on duty" refers to the period when an employee is performing an official duty or acting in an official capacity, whether or not the employee is being paid at the time (*e.g.*, misconduct occurring while an employee is driving a Secret Service vehicle home at the end of the employee's shift, is traveling on a commercial carrier while armed, or is on official travel status is considered "on duty" for administrative disciplinary purposes). • See the Penalty Guidelines for an expanded discussion of applicable penalties, including examples of mitigating and aggravating factors for various offenses.

1. MISSION RELATED MISCONDUCT	
Offense Code 1.1 Activities that Jeopardize the Secret Service Mission	**Engaging, assisting, or participating in an activity that jeopardizes or negatively impacts the Secret Service's mission or operations not specifically delineated in any other Offense Code.** **Mitigated: 5-10 Days** **Penalty: 14 Days** **Aggravated: 21 Days - Removal**
Offense Code 1.2 Asset/Cooperating Witness (CW)/Informant (Source) – Failure to Report Criminal Activity or Improper Intervention on Behalf Of	**Failing to inform in a timely manner the appropriate Secret Service official of a source's unauthorized criminal activity about which the employee knows, or reasonably should know, based upon all available information; or without authorization, aiding, protecting, harboring, or shielding a source, or any attempt to aid, protect, harbor, or shield a source from law enforcement or legal obligations. Timely manner means as soon as possible in light of operational/mission requirements.** "Criminal activity" does not include non-felonious traffic related offenses. **Mitigated: 1 – 5 Days** **Penalty: 7 Days** **Aggravated: 10 Days – Removal**

Offense Code 1.3 Asset/CW/Informant (Source) – Improper Relationship	**Without authorization, directly or indirectly loaning money to or receiving money from a source; giving a favor/gift to or accepting a favor/gift from a source; paying a source for a favor, gift, or service; attempting to obtain any favor, gift, or service from a source; or engaging in a social, romantic, sexual, or intimate relationship with a source.** This includes financial benefits, favors, and gifts conferred upon an employee's relatives or associates due to the employee's relationship with the source. Social relationships/associations involve any contact beyond that reasonably necessary for the completion of an investigative mission or beyond that which is authorized. An employee can be disciplined for: 1) engaging in an improper personal relationship, or 2) engaging in unauthorized conduct that would cause the reasonably prudent person to believe that there is an improper relationship. **Mitigated: 3 – 7 Days** **Penalty: 10 Days** **Aggravated: 14 Days – Removal**
Offense Code 1.4 Improper Handling of Document(s) or Property in the Care, Custody, or Control of the Government	**Intentionally failing to properly process, seize, describe, package, inventory, verify, record, document, control, store, secure, or safeguard documents or property under the care, custody, or control of the government, including evidence, counterfeit currency/notes/bonds, non-evidentiary items, or seized property held by the government.** This offense includes, but is not limited to, the unauthorized or improper use, loss, damage, destruction, or improper disposal of documents or property, to include electronic surveillance materials and classified or law enforcement sensitive documents. Note that the improper handling of classified information also raises security concerns and could result in a security clearance action. **Mitigated: Letter of reprimand – 3 Days** **Penalty: 5 Days** **Aggravated: 7 Days – 30 Days**
Offense Code 1.5 Leaving Post Without Proper Relief	**Without authorization, leaving an assignment without proper relief.** **Mitigated: Letter of reprimand – 3 Days** **Penalty: 5 Days** **Aggravated: 7 Days – 30 Days**
Offense Code 1.6 Misconduct Related to Judicial Proceedings	**During the investigative or litigation phases of a criminal or civil case, engaging in conduct that dishonors, discredits, or otherwise brings the integrity of the Secret Service into question.** This does not apply to conduct involving falsification covered under Offense Code 2.6, Lack of Candor/Lying - Under Oath. **Mitigated: 3 – 7 Days** **Penalty: 10 Days** **Aggravated: 14 Days – Removal**

Offense Code 1.7 Misconduct Related to Investigative or Protective Activities	**Recklessly disregarding rules governing search, seizure, arrest, treatment of suspects or individuals under arrest, or the exercise of an individual's constitutional rights.** See Federal Rules of Criminal Procedure, Rule 41. **Mitigated: 3 – 7 Days** **Penalty: 10 Days** **Aggravated: 14 – 30 Days**
Offense Code 1.8 Negligence in Performance of Official Duties	**Negligently performing your official duties.** Examples of negligent performance include, but are not limited to, sleeping or appearing to sleep while on duty, inattention to duty, using unauthorized electronic devices while on duty. **Mitigated: Letter of reprimand – 3 Days** **Penalty: 5 Days** **Aggravated: 7 - 21 Days**
Offense Code 1.9 Suspect/Criminal Element – Improper Relationship	**Without authorization, engaging in a social, romantic, sexual, or intimate relationship or association with a person the employee knew, or should have known, is involved in criminal activities, or is a suspect in a Secret Service investigation.** Social relationships or associations involve any contact beyond that reasonably necessary for the completion of an investigative mission or beyond that which is authorized. **Mitigated: 5-10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**
Offense Code 1.10 Violation of Operational Guidelines and Policies, Other	**Failing to enforce or comply with a Secret Service operational guideline or policy not specifically delineated in any of the other Mission Related Misconduct Offense Codes provided herein.** **Mitigated: Letter of reprimand – 3 Days** **Penalty: 5 Days** **Aggravated: 7 - 30 Days**

2. INTEGRITY/ETHICAL MISCONDUCT	
Offense Code 2.1 False/Misleading/Inaccurate Information – Employment/Security Document(s)	**Knowingly providing false, misleading, or inaccurate information in an employment-related or security-related document; or signing or attesting to the truthfulness of information provided in an employment-related or security-related document in reckless disregard of the accuracy or completeness of pertinent information contained therein.** Employment/security related documents include, but are not limited to, the Employment Application, Security Investigation Questionnaires, and other security clearance forms; Government Employees Training Acts forms; training records; Candidate Qualification forms; report of medical history; and other documents/forms which impact hiring, retention, transfer, promotion and award decisions. Note that knowingly providing false, inaccurate, or misleading information on a security-related document also raises security concerns and could result in a security clearance action. **Mitigated: 5 – 10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**
Offense Code 2.2 False/Misleading Information – Fiscal Matter(s)	**Knowingly providing false or misleading information in a fiscal-related document; or signing or attesting to the truthfulness of information provided in a fiscal-related document in reckless disregard of the accuracy or completeness of pertinent information contained therein**. Documents involving fiscal matters include, but are not limited to, Time and Attendance (T&A) records, documentation for Law Enforcement Availability Pay (LEAP) hours, travel vouchers, disbursement/expenditure forms, draft requests, expense forms, supporting documentation for leave purposes, insurance forms, benefits forms, and transfer documents. Additionally, failure to follow Secret Service policy on reporting Administratively Uncontrollable Overtime (AUO) hours is also covered by this offense code. **Mitigated: 5 - 10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**
Offense Code 2.3 False/Misleading Information – Investigative Activity	**Knowingly providing false or misleading information in an investigative document; or signing or attesting to the truthfulness of information provided in an investigative document in reckless disregard of the accuracy or completeness of pertinent information contained therein.** Documents involving investigative matters include, but are not limited to, Memorandum Reports, inserts, evidence control documents, and documentation of informant matters. **Mitigated: 5 – 10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**

Offense Code 2.4 False/Misleading Information – Other Official Matter(s)	**Knowingly providing false or misleading information in an official Secret Service document or an official document of another government agency; or signing or attesting to the truthfulness of information provided in an official Secret Service document or official document of another government agency in reckless disregard of the accuracy or completeness of pertinent information contained therein.** This applies to documents executed either on-duty or off-duty. **Mitigated: 5 – 10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**
Offense Code 2.5 Lack of Candor – No Oath	**Knowingly providing inaccurate information when making a verbal or written statement, not under oath, to a supervisor, another Secret Service employee in an authoritative position, or another governmental agency, when the employee is questioned about his/her conduct or the conduct of another person.** "Inaccurate information" includes misrepresentations, the failure to be fully forthright, or the concealment of a material fact/information. When facts merit, Offense Code 2.5 should be charged independently of the underlying misconduct. **Mitigated: 1 – 5 Days** **Penalty: 7 Days** **Aggravated: 10 – Removal**
Offense Code 2.6 Lack of Candor/Lying – Under Oath	**Knowingly providing false information in a verbal or written statement made under oath.** "False information" includes false statements, misrepresentations, the failure to be fully forthright, or the concealment of a material fact/information. When facts merit, Offense Code 2.6 should be charged independently of the underlying misconduct. **Mitigated: 60 – 120 Days** **Penalty: Removal** **Aggravated: N/A**
Offense Code 2.7 Misuse of Position	**Exceeding the limits of Secret Service authority to further a personal, unofficial, or unauthorized interest; or using Secret Service position or affiliation for private gain or advantage or for the gain or advantage of relatives or associates of the employee.** See 5 C.F.R. § 2635.702 for additional information. **Mitigated: Letter of reprimand – 3 Days** **Penalty: 5 Days** **Aggravated: 7 - 30 Days**

Offense Code 2.8 Failure to Cooperate in an Administrative Matter	**Failing or refusing to fully participate in an administrative matter after an employee has been provided with the administrative warnings (i.e., Kalkines Warnings).** "Administrative Matter" includes, but is not limited to, internal disciplinary investigations, OIG investigations, Inspection Division investigations, or EEO Matters. **Mitigated: 60 – 120 Days** **Penalty: Removal** **Aggravated: N/A**
Offense Code 2.9 Obstruction of an Administrative Matter	**Taking any action to influence, intimidate, impede or otherwise obstruct an administrative matter.** "Administrative Matter" includes, but is not limited to, internal disciplinary investigations, OIG investigations, Inspection Division investigations, or EEO Matters. **Mitigated: 3- 7 Days** **Penalty: 10 Days** **Aggravated: 14 Days – Removal**
Offense Code 2.10 Prohibited Personnel Practices	**Committing a prohibited personnel practice (5 U.S.C. 2302) not elsewhere covered in the Offense Codes provided herein.** See 5 U.S.C. § 2302 for information concerning prohibited personnel practices. **Mitigated: Letter of reprimand – 1 Day** **Penalty: 3 Days** **Aggravated: 5 Days –Removal**
Offense Code 2.11 Violation of Ethical Guidelines	Engaging in any activity or conduct prohibited by the Standards of Ethical Conduct for Employees of the Executive Branch, or Secret Service or DHS policy. Conduct covered by this charge includes, but is not limited to, conflicts of interest, the acceptance of gifts from outside sources, impartiality in the performance of official duties, misuse of position, and outside activities. See 18 USC 201, 203, 205, 208, 209; Executive Order 12,674; 5 CFR 2635; LEG-06(02) "Standards of Ethical, Professional, and Personal Conduct: A Desk Reference for Secret Service Employees," and additional sources cited therein. **Mitigated: Letter of reprimand** **Penalty: 5 Days** **Aggravated: 10 Days – Removal**

3. PROPERTY/RELATED MISCONDUCT	
Offense Code 3.1 Destruction or Improper Disposal of Government Property	**Without proper authority, damaging, destroying, or disposing of any government document(s) or property.** This does not include the destruction or wrongful disposal of the type of property and documents covered in Offense Code 1.4, Mission Related Misconduct, Improper Handling of Document(s) or Property. **Mitigated: Letter of reprimand - 3 Days** **Penalty: 5 Days** **Aggravated: 7- 14 Days**
Offense Code 3.2 Loss of Government Property or Document(s) of a Sensitive/Valuable Nature	**Loss or theft of government property, including documents, resulting from the employee's failure to adequately safeguard an item, deemed by an appropriate authority to be of a sensitive or valuable nature**. This includes loss or theft of a Secret Service Special Agent or Uniformed Division badge or Secret Service credentials. This does not include the loss of the type of property and documents covered in Offense Code 1.4, Mission Related Misconduct, Improper Handling of Document(s) or Property or the loss or theft of classified information which is covered by Offense Code, 3.3, Loss of Classified Information. **Mitigated: Letter of reprimand - 1 Day** **Penalty: 3 Days** **Aggravated: 5- 14 Days**
Offense Code 3.3 Loss of Classified Information	**Loss or theft of classified national security information, resulting from the employee's willful failure to adequately safeguard the information**. Refer to SCD-03(01). Note that the loss or theft of classified information also raises security concerns and could result in a security clearance action. **Mitigated: 3 - 7 Days** **Penalty: 10 Days** **Aggravated: 14 Days - Removal**
Offense Code 3.4 Loss of Firearm	**Loss or theft of a Secret Service official firearm resulting from employee's failure to adequately safeguard the property.** **Mitigated: 3 – 7 Days** **Penalty: 10 Days** **Aggravated: 14 – 30 Days**

Offense Code 3.5 Misuse of Secret Service Database(s)/Unauthorized Access	**Without authorization, accessing a Secret Service or other government database or record.** Examples of databases include but are not limited to NCIC, TECS, etc. This does not include the disclosure of such information to others, which is covered in Offense Code 4.12, Illegal/Criminal Misconduct, Unauthorized Disclosure – Classified/Law-Enforcement Sensitive/Grand Jury Information or Offense Code 4.13, Illegal/Criminal Misconduct, Unauthorized Disclosure - Sensitive Information **Mitigated: Letter of reprimand – 3 Days** **Penalty: 5 Days** **Aggravated: 7 Days – Removal**
Offense Code 3.6 Misuse of Government Computer(s)	**Using a government computer or other electronic device for personal, unofficial, or unauthorized use.** This does not include use of a classified system. This does not apply to *de minimis* use, i.e., where the cost to the government is negligible, as long as the use is not otherwise objectionable. See 5 C.F.R. § 2635.704, IRM-10(03), and ITG-03(06). **Mitigated: Letter of reprimand – 1 Day** **Penalty: 3 Days** **Aggravated: 5 – 14 Days**
Offense Code 3.7 Misuse of Government Computer(s) – Inappropriate Content	**Without authorization, using a government computer or electronic device to create, send, solicit, or view any material that is sexual in nature or that makes fun of or insults others' race, religion, color, sex, disability, national origin, or sexual orientation ("prohibited material").** The unintended receipt and viewing of prohibited material is not a violation of this Offense Code. **Mitigated: Letter of reprimand – 3 Days** **Penalty: 5 Days** **Aggravated: 7 Days – Removal**
Offense Code 3.8 Misuse of Secure Communication Systems	**Using a secure communication system for personal, unofficial, or unauthorized use.** Refer to SCD-03(01). Note that misuse of classified systems also raises security concerns and could result in a security clearance action. **Mitigated: 3 - 7 Days** **Penalty: 10 Days** **Aggravated: 14 Days – Removal**
Offense Code 3.9 Misuse of Government Charge Card – Personal Use	**Knowingly using or permitting the use of, a Government Charge Card (GCC) for personal purchase, rentals, services, and/or cash advance resulting in financial gain to the employee or others.** **Mitigated: 21 – 45 Days** **Penalty: Removal** **Aggravated: N/A**

Offense Code 3.10 Misuse of Government Vehicle Non-Title 31	**Using or permitting the use of, a government owned, leased, or rented passenger motor vehicle, boat, or aircraft, or the equipment therein, regardless of the employee's intent, for an unofficial purpose; or transporting or allowing another to transport an unauthorized passenger in a motor vehicle, boat, or aircraft.** **Mitigated: Letter of reprimand - 3 Days** **Penalty: 5 Days** **Aggravated: 7- 30 Days**
Offense Code 3.11 Misuse of Government Vehicle Title 31	**Knowingly or with reckless disregard, using or permitting the use of, a government owned or leased passenger motor vehicle, boat, or aircraft for an unofficial or purely personal purpose (i.e., a purpose other than the facilitation of government work or the execution of the Secret Service's mission).** See 31 U.S.C. §§ 1344 and 1349(b). **Mitigated: N/A** **Penalty: 30 Days** **Aggravated: 45 Days – Removal**
Offense Code 3.12 Misuse of Government Property, Other	**Using government property, not specifically delineated in another offense code, for personal, unofficial or unauthorized use.** This does not apply to *de minimis* use, where the cost to the government is negligible. See 5 C.F.R. § 2635.704. **Mitigated: N/A** **Penalty: Letter of reprimand** **Aggravated: 1-10 Days**

4. ILLEGAL/CRIMINAL CONDUCT	
Offense Code 4.1 Assault	**Attempting or threatening to inflict bodily harm on another using unlawful force or violence.** **Mitigated: 1 – 5 Days** **Penalty: 7 Days** **Aggravated: 10 Days – Removal**
Offense Code 4.2 Battery	**Inflicting bodily harm on another using unlawful force or violence.** **Mitigated: 5 – 10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**

Offense Code 4.3 Counterfeit Related Offenses	**Any activity which violates laws relating to the creation, passing, or uttering of counterfeit currency, notes, bonds, or other obligations of the United States.** **Mitigated: 21 – 45 Days** **Penalty: Removal** **Aggravated: N/A**
Offense Code 4.4 Domestic Violence – Law Enforcement Officers Domestic Violence – Non- Law Enforcement Personnel	**Conviction of a felony or misdemeanor act of domestic violence.** Applies to law enforcement officers only. Law enforcement officers include: Special Agents, Uniformed Division Officers, Physical Security Specialists, Special Officers, and Operation Support Technicians, Physical Security Technicians. An LEO convicted of a domestic violence offense will, at a minimum, be removed from his/her LEO position. See 18 U.S.C. §922(g)(9) and 5 U.S.C. § 7371. **Mitigated: 21 – 45 Days** **Penalty: Removal** **Aggravated: N/A** **Conviction of a non-law enforcement employee for felony or misdemeanor act of domestic violence.** **Mitigated: 21 – 45 Days** **Penalty: Removal** **Aggravated: N/A**
Offense Code 4.5 Drugs – Use or Possession	**Knowingly and consciously ingesting, injecting, inhaling, possessing, selling or distributing an illegal controlled substance or anabolic steroid, on or off duty, after entering on duty.** An illegal controlled substance includes all substances designated as such under Federal law. See 21 U.S.C. § 812 for a list of controlled substances. Note that marijuana is an illegal controlled substance under Federal law regardless of any State law initiatives which may permit recreational or medicinal use. This Offense Code does not apply to the possession of controlled substances for official purposes. **Mitigated: 21 – 45 Days** **Penalty: Removal** **Aggravated: N/A**
Offense Code 4.6 DUI/DWI – Government Vehicle	**Operating or being in actual physical control of government owned, leased, or rented passenger motor vehicle, boat, or aircraft, while intoxicated or impaired by alcohol or a controlled substance.** Impairment can be evidenced by a chemical analysis (breathalyzer and/or blood test), or credible observations of law enforcement personnel or other witnesses if no law enforcement personnel are present. **Mitigated: 30 – 40 Days** **Penalty: 45 Days** **Aggravated: Removal**

Offense Code 4.7 DUI/DWI – Privately Owned Vehicle, Law Enforcement Officer	**Operating or being in actual physical control of any privately owned, leased, or rented passenger motor vehicle, boat, or aircraft, while intoxicated or impaired by alcohol or a controlled substance.** This offense code applies to Law Enforcement officers. Law enforcement officers include: Special Agents, Uniformed Division Officers, Physical Security Specialists, Special Officers, and Physical Security Technicians. Impairment can be evidenced by a chemical analysis (breathalyzer and/or blood test), or credible observations of law enforcement personnel or other witnesses if no law enforcement personnel are present. **Mitigated: 5 - 10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**
Offense Code 4.8 DUI/DWI – Privately Owned Vehicle, Non-Law Enforcement Personnel	**Operating or being in actual physical control of any privately owned, leased, or rented passenger motor vehicle, boat, or aircraft, while intoxicated or impaired by alcohol or a controlled substance.** This offense code applies to non-Law Enforcement personnel. Impairment can be evidenced by a chemical analysis (breathalyzer and/or blood test), or credible observations of law enforcement personnel or other witnesses if no law enforcement personnel are present. **Mitigated: 1 – 5 Days** **Penalty: 7 Days** **Aggravated: 10 Days – Removal**
Offense Code 4.9 Fraud/Theft	**Taking, obtaining, or withholding, by any means, from the possession of the government or another owner, any money, property or article of value of any kind, with the intent to deprive or defraud the government or another owner, of the use and benefit of the property or with the intent to appropriate it for personal use of for the use of another entity or person other than the owner.** This does not include conduct covered under the Offense Codes included in Part 3, Property Related Misconduct. **Mitigated: 21 – 45 Days** **Penalty: Removal** **Aggravated: N/A**
Offense Code 4.10 Indecent/Lascivious Acts	**Inappropriately acting in a manner to appeal to or gratify the sexual desires of the employee, victim, or both; or intentionally exposing an intimate body part to public view.** This does not apply to sexual assault or any sexually related conduct rising to the level of a felony offense, as determined by the jurisdiction in which the act occurred, which is covered under 4.11, Other Felonies. **Mitigated: 10 -21 Days** **Penalty: 30 Days** **Aggravated: 45 Days – Removal**

Offense Code 4.11 Other Felonies	**Engaging in an act, other than one which has been specifically delineated in another offense code, which is considered a felony in the jurisdiction in which the act occurred**. This does not apply to perjury, which is covered under Offense Code 2.6, Lack of Candor/Lying- Under Oath. **Mitigated: 10 – 21 Days** **Penalty: 30 Days** **Aggravated: 45 Days – Removal**
Offense Code 4.12 Other Misdemeanors	**Engaging in an act, other than one which has been specifically delineated in another offense code, which is considered a misdemeanor in the jurisdiction in which the act occurred**. **Mitigated: 1 – 5 Days** **Penalty: 7 Days** **Aggravated: 10 – Removal**
Offense Code 4.13 Unauthorized Disclosure – Classified/Law-Enforcement Sensitive/Grand Jury Information	**Without authorization, disclosing or attempting to disclose classified, or law enforcement sensitive materials, or Grand Jury Information.** See the Federal Rules of Criminal Procedure, Rule 6(e), for additional information. Refer to SCD-03(01). Note that the loss or theft of classified information also raises security concerns and could result in a security clearance action. **Mitigated: 3 – 7 Days** **Penalty: 10 Days** **Aggravated: 14 Days – Removal**
Offense Code 4.14 Unauthorized Disclosure - Sensitive Information	**Without authorization, disclosing or attempting to disclose the Secret Service's, or another Agency's, sensitive material.** This also includes disclosures of information in violation of the Privacy Act of 1974, 5 U.S.C. § 552a. **Mitigated: 1 – 5 Days** **Penalty: 7 Days** **Aggravated: 10 Days – Removal**

5. GENERAL MISCONDUCT	
Offense Code 5.1 Absence Without Leave	**Absence Without Leave (AWOL) or unauthorized absence from work place.** **Mitigated: Letter of reprimand - 1 Day** **Penalty: 3 Days** **Aggravated: 5 Days – Removal**
Offense Code 5.2 Alcohol/Substance Abuse – Under the Influence While on Duty	**Without authorization, consuming a beverage containing alcohol while on duty or during a break; consuming alcohol prior to reporting for duty to the extent that it has an effect on the employee's workplace or performance; or using prescribed medicine in a manner inconsistent with the prescribing physician's instructions, having an effect on the employee's workplace or performance.** **Mitigated: 5 – 10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**
Offense Code 5.3 Alcohol/Substance Abuse – Consumption During Abstinence Period or at Prohibited Locations	**Consuming alcohol within any designated period of abstinence prior to reporting for duty; consuming alcohol at the protectee's hotel after a protective visit begins; or consuming more than a moderate amount of alcohol while off duty on TDY assignments.** **Mitigated: Letter of reprimand – 5 Days** **Penalty: 7 Days** **Aggravated: 10 Days – Removal**
Offense Code 5.4 Bias-Motivated Groups or Activities	**Becoming or remaining a member of, participating in activities or knowingly associating yourself with a hate group or the hate-motivated activities of others.** "Hate group" or "hate-motivated activities" include any organization, association, event, or activity whose sole or primary purpose is to advocate or promote hate, violence, or invidious prejudice against individuals on account of protected classes. See ITG-03(05). **Mitigated: 21 – 45 Days** **Penalty: Removal** **Aggravated: N/A**

Offense Code 5.5 Bias-Motivated Conduct or Behavior	**On or off duty, using offensive, abusive, derisive, profane, degrading, critical, or demeaning statements, remarks, comments, observations, or actions, conduct, or gestures based on another's protected group, including creating a hostile work environment based on protected group membership.** "Protected Group" includes race, color, religion, national origin, sex, age, disability, sexual orientation, protected genetic information, marital status, parental status. **Mitigated: Letter of reprimand - 3 Days** **Penalty: 5 Days** **Aggravated: 7 Days - Removal**
Offense Code 5.6 Dereliction of Supervisory Responsibility	**A supervisor, or an employee acting in an authorized supervisory capacity, failing to exercise reasonable care in the execution of his/her duties or responsibilities; disregarding his/her duties or responsibilities; significantly deviating from appropriate methods of supervision; or failing to follow Secret Service policy on review and certification of claimed Administratively Uncontrollable Overtime (AUO).** **Mitigated: Letter of reprimand - 3 Days** **Penalty: 5 Days** **Aggravated: 7-14 Days**
Offense Code 5.6A Dereliction of Supervisory Responsibility - Failure of Supervisor to Report Misconduct	**A supervisor, or an employee acting in an authorized supervisory capacity, intentionally failing to report an employee's misconduct involving violations set forth in the Table of Penalties; section SCD-02(01) relating to security policies and procedures; and other violations of law, regulation, or policy (see LEG-06(02), "Standards of Ethical, Professional, and Personal Conduct: A Desk Reference for Secret Service Employees."** This Offense Code does not require that supervisors report performance issues and other minor policy violations not otherwise described above. **Mitigated: N/A** **Penalty: Letter of reprimand** **Aggravated: 1-14 Days**
Offense Code 5.7 Disclosure of Information and Documents	**Intentional disclosure of sensitive information obtained during course of employment with the Secret Service including information obtained from a protectee, observations of a protectee, sensitive but unclassified information, or Secret Service documents without permission.** **Mitigated: 1 – 5 Days** **Penalty: 7 Days** **Aggravated: 10 Days – Removal**

Offense Code 5.8 Discrimination/Harassment	**Acting or failing to act on an official matter in a manner which improperly takes into consideration an individual's protected group; failing to take appropriate action to prevent or curtail prohibited discrimination or harassment of a subordinate when the supervisor knew or should have known the conduct was discriminatory.** "Protected Group" includes race, color, religion, national origin, sex, disability, age, parental status, sexual orientation, protected genetic information, marital status, parental status, or political affiliation. See, e.g., Civil Rights Act of 1964; Age Discrimination in Employment Act; and Executive Order 11478. **Mitigated: 10 – 21 Days** **Penalty: 30 Days** **Aggravated: 45 Days – Removal**
Offense Code 5.9 Discourteous Conduct	**Using rude, impolite, discourteous, disrespectful, unprofessional, foul, derogatory, or similarly inappropriate language, gestures, or other conduct to or about another employee or members of the public while on duty or acting in an official capacity.** **Mitigated: Letter of reprimand - 1 Day** **Penalty: 3 Days** **Aggravated: 5 Days – Removal**
Offense Code 5.10 Disruptive Behavior	**Fighting, threatening, intimidating, attempting to inflict, or inflicting bodily harm to another; harassing or provoking quarrel; engaging in dangerous horseplay; any violent, reckless, or disorderly act, language, gestures, or conduct toward other employees or members of the public.** **Mitigated: Letter of reprimand - 3 Days** **Penalty: 5 Days** **Aggravated: 7 Days - Removal**
Offense Code 5.11 Failure to Follow Appearance Policy	**Failure to maintain a neat, clean, professional, and business-like appearance; failure to comply with uniform or appearance standards while on duty, on official travel, or (if a Law Enforcement Officer) traveling while armed in a non-duty status.** Note, this does not include instances where an accommodation has been granted. See ITG-03(05) for the Appearance Standards for Secret Service employees. **Mitigated: Letter of reprimand - 1 Day** **Penalty: 3 Days** **Aggravated: 5 Days – Removal**
Offense Code 5.12 Failure to Follow Instructions	**Failure to promptly and fully comply with lawful directions, instructions, or assignments of a supervisor or other management official; failure to follow a regulation, policy, procedure, practice, protocol or rule.** **Mitigated: Letter of reprimand - 1 Day** **Penalty: 3 Days** **Aggravated: 5 – 7 Days**

Offense Code 5.13 Failure to Follow Leave Policies	**Failure to follow established leave procedures including while on leave restriction or on administrative leave; improper use of sick leave or other leave programs; excessive unscheduled absences.** **Mitigated: Letter of reprimand - 1 Day** **Penalty: 3 Days** **Aggravated: 5 Days – Removal**
Offense Code 5.14 Failure to Honor Just Debts/Regulatory Obligations	**Without valid justification, failing to satisfy an uncontested, lawful debt, or to fulfill legal or regulatory obligation.** The failure to satisfy the debt or fulfill the obligation must be characterized by deceit, evasion, false promises, or other indicators of a deliberate nonpayment or gross indifference towards the just debt or obligation. This does not apply to debts involving government credit cards, which are covered under Offense Code 3.7, Misuse of Government Charge Cards – Personal Use, or Failure to file and/or pay any Federal, state, or local tax obligation which is covered by Offense Code 5.14A. Note that Failure to Honor Just Debts also raises security concerns and could result in a security clearance action. **Mitigated: 3 – 7 Days** **Penalty: 10 Days** **Aggravated: 14 Days – Removal**
Offense Code 5.14A Failure to File any Federal, state, or local tax obligation	**Without valid justification, failing to file any Federal, state, or local tax obligation.** **Mitigated: Letter of reprimand – 1 Day** **Penalty: 3 Days** **Aggravated: 5 Days – Removal**
Offense Code 5.15 Failure to Maintain Top Secret Security Clearance – Final Revocation	**Failure to maintain your Top Secret Security Clearance resulting in its final revocation.** See Human Resources Manual section RPS-02(02) or its successor sections. **Mitigated: N/A** **Penalty: Removal** **Aggravated: N/A**
Offense Code 5.16 Failure to Maintain Top Secret Security Clearance – Revocation or Suspension/Denial of Eligibility for Access to Classified Information	**Failure to maintain a Top Secret Security Clearance resulting in its revocation or a denial of eligibility for access classified information.** See Human Resources Manual section RPS-02(02) or its successor sections. **Mitigated: Approved Leave Status** **Penalty: Indefinite Suspension** **Aggravated: N/A**

Offense Code 5.17 Failure to Report	**Failing to inform the appropriate Secret Service official or supervisor, and the Security Clearance Division, in a timely manner, about a matter concerning the employee which the employee knew, or should have known, was required by Secret Service policy to be reported, including foreign contacts and foreign travel.** Refer to SCD-02(01) for additional information. Note that this offense does not include failure to report criminal or serious misconduct by the employee which is covered by Offense Code 5.18, Failure to Report – Criminal/Serious Misconduct. **Mitigated: N/A** **Penalty: Letter of reprimand** **Aggravated: 1- 10 Days**
Offense Code 5.17A Failure to Report – Loss of Property	**Intentional failure to inform the appropriate Secret Service official or supervisor, in a timely manner, about a matter concerning a loss of equipment/weapon which the employee knew, or should have known, was required by Secret Service policy to be reported.** **Mitigated: Letter of reprimand to 3 Days** **Penalty: 5 Days** **Aggravated: 7- 14 Days**
Offense Code 5.17B Failure to Submit Required Documents	**Intentional failure to timely submit required forms or attend required Ethics training.** This offense includes failure to submit required security clearance documents, medical documentation (Medical Review Board documents), and ethics forms (See 5 CFR 2638.704, 2638.705). **Mitigated: N /A** **Penalty: Letter of reprimand** **Aggravated: 5 Days**
Offense Code 5.18 Failure to Report – Criminal/Serious Misconduct	**Failing to inform the appropriate Secret Service official or supervisor, in a timely manner, about any serious misconduct the employee committed; any arrest, summons, contact with law enforcement, or involvement in the court system by the employee; or any serious misconduct or criminal conduct committed by another employee of which the employee was aware and of which the employee is also aware was not otherwise reported.** Refer to SCD-02(01) for additional information. **Mitigated: Letter of reprimand – 3 Days** **Penalty: 5 Days** **Aggravated: 7 -14 Days**
Offense Code 5.19 Insubordination	**After being given a legitimate order, made orally or in writing, by a supervisor or another person in authority, intentionally or willfully failing to comply with the order.** **Mitigated: 5 – 10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**

Offense Code 5.20 Misuse of Weapon – Storage	**Inappropriate storage, care, or misplacement of a weapon, explosive, incendiary device, or ammunition.** This offense does not include the loss or theft of a firearm which is covered by Offense Code 3.4, Loss or Theft of Firearm. **Mitigated: Letter of reprimand – 3 Days** **Penalty: 5 Days** **Aggravated: 7 Days – Removal**
Offense Code 5.21 Misuse of Weapon – Display	**Inappropriate handling, displaying, operating, brandishing, or otherwise displaying a weapon, explosive, or incendiary device in a manner inconsistent with the use and safety protocols and procedures established by the Secret Service and federal regulatory agencies.** **Mitigated: 1 – 5 Days** **Penalty: 7 Days** **Aggravated: 10 Days – Removal**
Offense Code 5.22 Misuse of Weapon – Negligent Discharge	**Causing the unintentional discharge of a weapon.** **Mitigated: Letter of reprimand** **Penalty: 1 Day** **Aggravated: 3-14 Days**
Offense Code 5.23 Misuse of Weapon – Intentional Discharge	**Purposefully or willfully discharging a weapon in violation of the use of force policy.** **Mitigated: 10 - 21 Days** **Penalty: 30 Days** **Aggravated: 45 Days – Removal**
Offense Code 5.24 Reasonable Cause to Believe Crime Has Been Committed	**Engaging in conduct which provides reasonable cause to believe that a crime has been committed for which a term of imprisonment may result.** "Reasonable cause" includes but is not limited to a criminal indictment or the acceptance of a case for criminal prosecution. Note that this offense also raises security concerns and could result in a security clearance action. **Mitigated: N/A** **Penalty: Indefinite Suspension** **Aggravated: N/A**
Offense Code 5.25 Retaliation	**Taking, or threatening to take, an adverse employment action against an employee who made, or was believed to have made, a protected disclosure, or who engaged, or who was believed to have engaged in a protected activity.** See, e.g., Whistleblower Protection Act; Whistleblower Protection Enhancement Act of 2012; Civil Rights Act of 1964; and any other anti-retaliation provisions of federal law. **Mitigated: 10 – 21 Days** **Penalty: 30 Days** **Aggravated: 45 Days – Removal**

Offense Code 5.26 Security Violation (Second Offense)	**Failing to safeguard or control access to non-public Secret Service space, to sensitive or classified material, or to the equipment or location where such material is inputted, maintained, collected, stored, or preserved after having received a prior security violation memorandum.** This does not apply to items covered in Offense Code 1.4, Improper Handling of Document(s) or Property in the Care, Custody, or Control of the Government. Note that this offense also raises security concerns and could result in a security clearance action. **Mitigated: Letter of reprimand** **Penalty: 1 Day** **Aggravated: 3 – 14 Days**
Offense Code 5.27 Sexual Misconduct - Consensual	**Engaging in sexual, intimate, or romantic activity in an inappropriate location (such as government spaces, government vehicles), or while on duty.** **Mitigated: 5-10 Days** **Penalty: 14 Days** **Aggravated: 21 Days – Removal**
Offense Code 5.28 Sexual Harassment	**Making unwelcome or unwanted sexual advances, requesting sexual favors, or engaging in other verbal or physical conduct of a sexual nature.** Unwelcome conduct of a sexual nature by a supervisor or coworker can constitute sexual harassment. See the Civil Rights Act of 1964, Title VII, §703, for additional information. **Mitigated: 10 – 21 Days** **Penalty: 30 Days** **Aggravated: 45 – Removal**
Offense Code 5.29 Solicitation or Payment for Sexual Services	**Solicitation of a prostitute or the exchange of money or items of value for sexual services regardless of whether the payment is made or negotiated prior to the act.** The fact that prostitution is legal in a particular location does not prevent the Agency from taking a disciplinary action under this Offense Code. The fact that an employee did not intend to pay for sexual services at the time they were rendered does not prevent the Agency from taking a disciplinary action under this Offense Code. Note this conduct may also raise security concerns and could result in a security clearance action. **Mitigated: 14 - 30 Days** **Penalty: 45 Days** **Aggravated: Removal**
Offense Code 5.30 Striking	**Engaging or encouraging a strike, work stoppage/slowdown, or sick out. See 5 U.S.C. § 7311.** **Mitigated: N/A** **Penalty: Removal** **Aggravated: N/A**

Offense Code 5.31 Unprofessional Conduct – Off Duty	**Engaging in conduct, while off duty, which dishonors, disgraces or discredits the Secret Service; seriously calls into question the judgment or character of the employee; or compromises the standing of the employee among his peers or his community.** This applies to misconduct not otherwise specifically delineated in any other Offense Code. **Mitigated: Letter of reprimand - 3 Days** **Penalty: 5 Days** **Aggravated: 7 Days- Removal**
Offense Code 5.32 Unprofessional Conduct – On Duty	**Engaging in conduct, while on duty or while in a travel status, which dishonors, disgraces, or discredits the Secret Service; seriously calls into question the judgment or character of the employee; or compromises the standing of the employee among his peers or his community.** This applies to misconduct not otherwise specifically delineated in any other Offense Code. **Mitigated: 1 – 5 Days** **Penalty: 7 Days** **Aggravated: 10 Days– Removal**
Offense Code 5.33 Unauthorized Recording	**Unauthorized recording or monitoring of telephone calls, meetings, conversations, emails, and things of a similar nature.** This offense does not include instances where such conduct could be considered a criminal violation covered by Offense Code 4.11 Other Felonies or 4.12 Other Misdemeanors. **Mitigated: 3 – 7 Days** **Penalty: 10 Days** **Aggravated: 14 Days – Removal**
Offense Code 5.34 Unavailability for Unscheduled Duty	**Unable to perform unscheduled duty for an extended period of time due to physical or health reasons, or failure to perform unscheduled duty (availability or work) as assigned or reported.** See 5 C.F.R. § 550.184. This does not apply to falsification or inaccurate reporting of LEAP hours which is covered by Offense Code 2.2 False/Misleading Information – Fiscal Matter(s). This Offense only applied to employees who receive LEAP. **Mitigated: N/A** **Penalty: Cancellation of LEAP** **Aggravated: N/A**
Offense Code 5.35 Violation of Miscellaneous Rules/Regulations	**Engaging in an activity or conduct in violation of, or failing to enforce or comply with a Secret Service, DHS, Office of Personnel Management, or other federal administrative or operational guideline or policy not specifically delineated in any other Offense Code.** **Mitigated: Letter of reprimand - 3 Days** **Penalty: 5 Days** **Aggravated: 7 – 30 Days**

Appendix B:
United States Secret Service Table of Penalties
(Penalty Guidelines – Applicable to Secret Service's Internal Disciplinary Process)

Penalty Guidelines – Applicable to Secret Service's Internal Disciplinary Process
• The listed penalties apply to all Secret Service personnel, regardless of position or title, except that Federal law prohibits an agency from taking a suspension action of less than 15 days against a Senior Executive Service (SES) employee (5 C.F.R. §752.601). In keeping with that requirement, the Introduction to the Table of Penalties provides that if a non-SES employee would have received a three-day suspension, the Deciding Official may impose on an SES employee a letter of reprimand or a minimum 15-day suspension, based on the Deciding Official weighing of the facts and circumstances of the case against the heightened behavioral and managerial expectations associated with SES personnel. • See the Offense Codes for a description of the behavior or actions that define the offenses.

1. MISSION RELATED MISCONDUCT

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 1.1	Activities that Jeopardize the Secret Service Mission	5 – 10 days (minimal financial impact)	14 days	21 days – Removal (personal injury or property damage; significant financial impact)
Penalty Guideline 1.2	Asset/Cooperating Witness (CW)/ Informant/ Source – Failure to Report Criminal Activity or Improper Intervention on Behalf of	1 – 5 days (No personal gain; good faith attempt to help source)	7 days	10 days – Removal (Compromise case or other cases; seriousness of criminal activity; financial benefit to employee; non-disclosure to AUSA)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 1.3	Asset/CW/Informant/ Source – Improper Relationship	3 – 7 days (No personal gain; good faith attempt to help source; lack of initial knowledge the individual was a source)	10 days	14 days – Removal (Financial benefit to employee; non-disclosure to AUSA)
Penalty Guideline 1.4	Improper Handling of Document(s) or Property in the Care, Custody, or Control of the Government	Letter of reprimand – 3 days (Others contributed to improper handling; inadvertent; exigent circumstances)	5 days	7 – 30 days (Significant loss of document(s)/property; intentional; compromise of case or mission)
Penalty Guideline 1.5	Leaving Post Without Proper Relief	Letter of reprimand – 3 days (exigent circumstances)	5 days	7 – 30 days (intentional disregard for safety of protectee or mission; failure to seek relief)
Penalty Guideline 1.6	Misconduct Related to Judicial Proceedings	3 – 7 days (Acted in good faith; inadvertent; no personal gain)	10 days	14 Days – Removal (Judicial criticism; significant impact on case; intentional)
Penalty Guideline 1.7	Misconduct Related to Investigative or Protective Activities	3 – 7 days (Acted in good faith inadvertent; no personal gain)	10 days	14 – 30 days (Judicial criticism; significant impact on case; intentional; damage to persons or property)
Penalty Guideline 1.8	Negligence in Performance of Official Duties	Letter of reprimand – 3 days (minimal impact on mission; exigent circumstances)	5 days	7 – 21 days (disruption of the mission)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 1.9	Suspect/Criminal Element – Improper Relationship	5 – 10 days (lack of initial knowledge the individual's criminal activity)	14 days	21 days - Removal (investigation or prosecution impacted; future or past cases impacted of Secret Service or another LE agency)
Penalty Guideline 1.10	Violation of Operational Guidelines and Policies, Other	Letter of reprimand – 3 days (unintentional)	5 days	7 – 30 days (Jeopardizing safety of others; the mission; a prosecution or investigation)

2. INTEGRITY/ETHICAL MISCONDUCT

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 2.1	False/Misleading Information – Employment/Security Document(s)	5 – 10 days (Minor issues that were immaterial to a hiring/security decision; failure to report mental health treatment)	14 days	21 days – Removal (Drugs, criminal activity, foreign contacts; or otherwise material to hiring/security decision)
Penalty Guideline 2.2	False/Misleading Information – Fiscal Matter(s)	5 – 10 days (Minor issues; little benefit to employee)	14 days	21 days – Removal (Serious T&A abuse; serious LEAP abuse; serious AUO abuse, significant benefit to employee; involving others; NOTE: voucher fraud warrants Removal)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 2.3	False/Misleading Information – Investigative Activity	5 – 10 days (Unintentional; minor issues; no material effect on agency/mission)	14 days	21 days – Removal (Intentional; significant issues; material impact on investigation/case; jeopardizing safety of others; causing use of additional resources Intentional)
Penalty Guideline 2.4	False/Misleading Information – Other Official Matter(s)	5 – 10 days (Unintentional no material effect on agency/mission)	14 days	21 days – Removal (Intentional and particularly material; released to another government agency or Congress)
Penalty Guideline 2.5	Lack of Candor/Lying – No Oath	1 – 5 days (Relatively insignificant matters)	7 days	10 days – Removal (Jeopardizing safety of others; causing use of additional resources; intentional; fact was material or central to the investigation, matter, or event about which the statement was made (e.g., misrepresentation to investigator in regard to fact material or central to investigation); released to another government agency or Congress)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 2.6	Lack of Candor/Lying – Under Oath	60 – 120 days (No impact on the safety of others; no additional resources used; no impact on mission; fact was not material or central to the investigation, matter, or event about which the statement was made (e.g., misrepresentation to investigator in regard to fact that was not material or central to investigation))	Removal	N/A
Penalty Guideline 2.7	Misuse of Position	Letter of reprimand – 3 days (Doing so to prevent harm to another or to ensure safety of public/others; minor issue; minimal benefit)	5 days	7 – 30 days (Uncooperative; confrontational; display of weapon; safety hazard; security issue; financial gain; threatening or aggressive behavior)
Penalty Guideline 2.8	Failure to Cooperate in an Administrative Matter	60 – 120 days (Eventually cooperated and there was no impact on the safety of others; no additional resources used; no impact on mission)	Removal	N/A
Penalty Guideline 2.9	Obstruction of an Administrative Matter	3 – 7 days (unintentional)	10 days	14 days - Removal (Threatening or aggressive behavior; intimidating a witness)
Penalty Guideline 2.10	Prohibited Personnel Practices	Letter of reprimand – 1 day (unintentional; no personal gain)	3 days	5 days – Removal (interfering with promotions or hiring)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 2.11	Violation of Ethical Guidelines	Letter of reprimand (No personal gain; good faith attempt to assist another)	5 days	10 days – Removal (Financial gain; duration; direct/obvious conflict; impact on agency/mission)

3. PROPERTY/RELATED MISCONDUCT

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 3.1	Destruction or Improper Disposal of Government Property	Letter of reprimand - 3 days (Minimal, insignificant value of property)	5 days	7 – 14 days (Significant value of property; personal gain; weapon)
Penalty Guideline 3.2	Loss of Government Property or Document(s) of a Sensitive/Valuable Nature	Letter of reprimand - 1 day (Minimal, insignificant value; minimal impact on agency/mission; prompt reporting)	3 days	5 – 14 days (Significant value of property; compromise investigation; repeated loss; failure to promptly report)
Penalty Guideline 3.3	Loss of Classified Information	3 – 7 days (Minimal impact on agency/mission; prompt reporting)	10 days	14 days – Removal (Significant impact on agency/mission; failure to promptly report)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 3.4	Loss of Firearm	3 – 7 days (prompt reporting; exigent circumstances)	10 days	14 – 30 days
Penalty Guideline 3.5	Misuse of Secret Service Database(s)/ Unauthorized Access	Letter of reprimand - 3 days (Non-sensitive information; NOTE: no mitigation for NCIC, TECS or other LEO database with criminal penalties for misuse)	5 days	7 days – Removal (Duration; frequency; type of information obtained/accessed; personal gain/use)
Penalty Guideline 3.6	Misuse of Government Computer(s)	Letter of reprimand – 1 day (Minimal use/duration)	3 days	5 – 14 days (Duration; frequency; type of information obtained/accessed)
Penalty Guideline 3.7	Misuse of Government Computer(s) – Inappropriate Material	Letter of reprimand – 3 days	5 days	7 days – Removal (Frequency; numerous recipients; sent outside the Agency; repeated misuse)
Penalty Guideline 3.8	Misuse of Secure Communications Systems	3 – 7 days (No impact on agency mission)	10 days	14 days – Removal (Frequency)
Penalty Guideline 3.9	Misuse of Government Charge Card – Personal Use	21 – 45 days (Expeditious self-reporting of unintentional or emergency use; minimal dollar amount charged)	Removal	N/A

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 3.10	Misuse of Government Vehicle, Non-Title 31	Letter of reprimand – 3 days (minimal use and duration)	5 days	7 – 30 days (Frequency; duration; accident; injury/harm to persons/property; citation/arrest/other violation of law, rule or regulation)
Penalty Guideline 3.11	Misuse of Government Vehicle, Title 31	N/A	30 Days	45 days – Removal (Frequency; duration; accident; injury/harm to persons/property; citation/arrest/other violation of law, rule or regulation)
Penalty Guideline 3.12	Misuse of Government Property, Other	N/A	Letter of reprimand	1 – 10 days (Frequency; duration; high value amount)

4. ILLEGAL/CRIMINAL CONDUCT

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 4.1	Assault	1 – 5 days (Provocation; defense of self or others)	7 days	10 days – Removal (Arrest/indictment/ Conviction; extent of injuries; alcohol-related; on-duty; criminal charges filed)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 4.2	Battery	5 -10 Days (Provocation; no physical injuries; defense of self or others)	14 Days	21 days – Removal (Child abuse; extent of injuries; alcohol-related; domestic violence – no conviction; on duty; arrest/indictment/ conviction)
Penalty Guideline 4.3	Counterfeit Related Offenses	21 – 45 days (non-LEO)	Removal (LEO)	N/A
Penalty Guideline 4.4	Domestic Violence Law Enforcement Officers Domestic Violence Non-Law Enforcement Personnel	21 – 45 days (no physical injuries, self-defense, provocation) 21 – 45 days (no physical injuries, self-defense, provocation)	Removal Removal	N/A N/A
Penalty Guideline 4.5	Drugs – Use or Possession	21 – 45 days (Minimal occurrence in distant past)	Removal	N/A
Penalty Guideline 4.6	DUI/DWI – Government Vehicle	30 – 40 days (first DUI/DWI; no personal injury or property damage)	45 days	Removal (Accident, injury, death; Arrest/indictment/ Conviction) NOTE: second occurrence may result in Removal

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 4.7	DUI/DWI – Privately Owned Vehicle, Law Enforcement Officer	5 – 10 days (first DUI/DWI; no personal injury or property damage)	14 days	21 days – Removal (Accident, injury, death; arrest/indictment/ Conviction) NOTE: third occurrence may result in Removal
Penalty Guideline 4.8	DUI/DWI – Privately Owned Vehicle, Non-Law Enforcement Personnel	1 – 5 days (first DUI/DWI; no personal injury or property damage)	7 days	10 days – Removal (Accident, injury, death; repeated occurrence; arrest/indictment/ conviction)
Penalty Guideline 4.9	Fraud/Theft	21 – 45 days (minimal value; off duty)	Removal	N/A
Penalty Guideline 4.10	Indecent/Lascivious Acts	10 – 21 days (off-duty; private location)	30 days	45 days – Removal (on duty; public location; complaints; child victim; arrest/indictment/ conviction)
Penalty Guideline 4.11	Other Felonies	10 – 21 days	30 days	45 days – Removal (Arrest/indictment/ conviction; injury/harm to persons/property; child victim)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 4.12	Other Misdemeanors	1 – 5 days	7 days	10 days – Removal (Arrest/indictment; conviction; injury/harm to persons/property; child victim)
Penalty Guideline 4.13	Unauthorized Disclosure – Classified/Law-Enforcement Sensitive/Grand Jury Information	3 – 7 days (Unintentional; minimal impact on agency/mission)	10 days	14 days – Removal (Compromise of case; jeopardizes safety of others; sensitivity of information; security issues; intentional; personal gain)
Penalty Guideline 4.14	Unauthorized Disclosure - Sensitive Information	1 – 5 days (Unintentional; minimal impact on agency/mission)	7 days	10 days – Removal (Compromise of case; jeopardizes safety of others; sensitivity of information; security issues; intentional; personal gain)

5. GENERAL MISCONDUCT

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 5.1	AWOL	Letter of reprimand – 1 day (exigent circumstances; limited time period – less than a full day; timely self- reporting)	3 days	5 days – Removal (Repeated occurrences; AWOL for a full work day or more)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 5.2	Alcohol/Substance Abuse – Under the Influence While on Duty	5 – 10 days (called into duty unscheduled and limited prior consumption)	14 days	21 days – Removal (Weapons involved; supervisory position; brought alcohol into workplace; extent of intoxication; injury/harm to persons/property; disruption of the workplace)
Penalty Guideline 5.3	Alcohol/Substance Abuse – Consumption During Abstinence Period or at Prohibited Locations	Letter of reprimand – 5 days (inadvertence; consumption in close proximity to abstinence period)	7 days	10 days – Removal (engaging in in appropriate behavior; level of intoxication; supervisory position)
Penalty Guideline 5.4	Bias-Motivated Groups or Activities	21 – 45 days (minimal participation; distant past)	Removal	N/A
Penalty Guideline 5.5	Bias-Motivated Conduct or Behavior	Letter of reprimand – 3 days (unintentional)	5 days	7 days – Removal (frequency; public nature; pervasiveness; previously warned; severity)
Penalty Guideline 5.6	Dereliction of Supervisory Responsibility	Letter of reprimand – 3 days (minimal impact on agency mission; no harm to persons or property; inadvertent)	5 days	7 – 14 days (Jeopardizes safety of others; injury/harm to persons/property; impact on agency/mission)
Penalty Guideline 5.6A	Dereliction of Supervisory Responsibility - Failure of Supervisor to Report Misconduct	N/A	Letter of reprimand	1 – 14 days (Jeopardizes safety of others; injury/harm to persons/property; impact on agency/mission)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 5.7	Disclosure of Information and Documents	1 – 5 days (minimal impact on agency mission; no harm to persons or property; inadvertent)	7 days	10 days – Removal (Jeopardizes safety of others; injury/harm to persons/property; impact on agency/mission; personal gain)
Penalty Guideline 5.8	Discrimination/ Harassment	10 – 21 days (minimal involvement; limited duration; not severe or pervasive)	30 days	45 days – Removal (Supervisory position; pervasiveness; duration; frequency; severity; multiple victims; previously warned)
Penalty Guideline 5.9	Discourteous Conduct	Letter of reprimand – 1 day (unintentional; private setting)	3 days	5 days – Removal (Supervisory position; pervasiveness; duration; frequency; severity; multiple victims; previously warned; public setting)
Penalty Guideline 5.10	Disruptive Behavior	Letter of reprimand – 3 days (unintentional; private setting)	5 days	7 days – Removal (On duty; in uniform; supervisory position; duration; frequency; severity; previously warned; public setting)
Penalty Guideline 5.11	Failure to Follow Appearance Policy	Letter of reprimand – 1 day (inadvertent)	3 days	5 days – Removal (Frequency; Willfulness; previously warned)
Penalty Guideline 5.12	Failure to Follow Instructions	Letter of reprimand – 1 day (unintentional; lack of understanding)	3 days	5 – 7 days (Willful; intentional; repeated behavior; instructed several times or instructions clarified)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 5.13	Failure to Follow Leave Policies	Letter of reprimand – 1 day (unintentional)	3 days	5 days – Removal (Repeated)
Penalty Guideline 5.14	Failure to Honor Just Debts/Regulatory Obligations	3 – 7 days (Took steps to resolve matter prior to discovery; minimal debt and prompt payment plan initiated)	10 days	14 days – Removal (Amount of debt; violation of court order; pattern; duration; frequency) NOTE: repeated or serious failure to pay Federal, state, or local taxes could result in Removal
Penalty Guideline 5.14A	Failure to File any Federal, state, or local tax obligation	Letter of reprimand - 1 Day (resulted in a refund to employee)	3 Days	5 Days – Removal (Resulted in employee owing money)
Penalty Guideline 5.15	Failure to Maintain Top Secret Security Clearance – Final Revocation	N/A	Removal	N/A
Penalty Guideline 5.16	Failure to Maintain Top Secret Security Clearance – Revocation or Suspension/ Denial of Eligibility to Access Classified Information	Approved Leave Status (mental health issue)	Indefinite Suspension (criminal or other serious violation alleged; Notice of Determination Issued)	N/A
Penalty Guideline 5.17	Failure to Report	N/A	Letter of reprimand	1 – 10 days (Willful; significant security issues; impact on agency/mission)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Offense Code 5.17A	Failure to Report – Loss of Property	Letter of reprimand – 3 days	5 days	7 – 14 days (Willful; significant security issues; impact on agency/mission)
Offense Code 5.17B	Failure to Submit Required Documents	N /A	Letter of reprimand	5 days (Willful; impact on agency/mission)
Penalty Guideline 5.18	Failure to Report – Criminal/Serious Misconduct	Letter of reprimand – 3 days (inadvertent)	5 days	7 – 14 days (Willful; seriousness of incident; significant security issues; impact on agency/mission; continuing)
Penalty Guideline 5.19	Insubordination	5 – 10 days (Reasonable belief order was unlawful or in violation of rule, regulation or policy)	14 days	21 days – Removal (Jeopardize safety to others; injury/harm to persons/property; impact on agency/mission; compromise of investigation)
Penalty Guideline 5.20	Misuse of Weapon - Storage	Letter of reprimand – 3 days (prompt reporting; exigent circumstances)	5 days	7 days – Removal (Repeated; other violation of law, rule or regulation involved; failure to promptly report; personal injury or property damage; level of safety risk)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 5.21	Misuse of Weapon - Display	1 – 5 days (exigent circumstances)	7 days	10 days – Removal (Intentional; level of safety risk; used to intimidate or threaten; altered weapon rendering more unsafe)
Penalty Guideline 5.22	Misuse of Weapon – Negligent Discharge	Letter of reprimand	1 day	3 – 14 days (Injury/harm to persons/property; violation of weapons law, regulation or policy)
Penalty Guideline 5.23	Misuse of Weapon – Intentional Discharge	10 – 21 days (Doing so to prevent harm to another or to ensure safety of public/others- no injury to persons or property)	30 days	45 days – Removal (Injury/harm to persons/property; violation of weapons law or regulation)
Penalty Guideline 5.24	Reason to Believe a Crime Has Been Committed	N/A	Indefinite Suspension	N/A
Penalty Guideline 5.25	Retaliation	10 – 21 days (No tangible employment action taken; minimal involvement; no adverse finding against the agency)	30 days	45 days – Removal (Liability imputed to the agency. EEOC/Court finding of retaliation; multiple victims)
Penalty Guideline 5.26	Security Violation (Second Offense)	Letter of reprimand (Minimal impact on agency/mission; insignificant matter; expeditious self-reporting; unintentional)	1 day	3 – 14 days (Compromise of case; impact on agency/mission; frequency; duration; severity; injury/harm to persons/property; jeopardize the safety of others; intentional)

Number	Offense	Mitigated Range	Standard Penalty	Aggravated Range
Penalty Guideline 5.27	Sexual Misconduct - Consensual	5 – 10 days (Minimal impact on agency/mission; insignificant matter)	14 days	21 days – Removal (Pervasiveness; impact on agency/mission; public nature)
Penalty Guideline 5.28	Sexual Harassment	10 – 21 days (initially consensual; unintentional; minimal involvement; limited duration; not severe or pervasive)	30 days	45 days – Removal (Pervasiveness; impact on agency/mission; impact on victim; EEOC or Court finding against the Agency)
Penalty Guideline 5.29	Solicitation	14 – 30 days (Non-law enforcement personnel; legal; off-duty)	45 days	Removal (Law enforcement officer; illegal; on-duty; on mission related travel)
Penalty Guideline 5.30	Striking	N/A	Removal	N/A
Penalty Guideline 5.31	Unprofessional Conduct – Off Duty	Letter of reprimand – 3 days (Minor incident; private setting; minimal mission/agency impact)	5 days	7 days – Removal (public nature; seriousness of the incident; impact on agency mission)
Penalty Guideline 5.32	Unprofessional Conduct – On Duty	1 – 5 days (Minor incident; private setting; minimal mission/agency impact)	7 days	10 days – Removal (public nature; seriousness of the incident; impact on agency mission)
Penalty Guideline 5.33	Unauthorized Recording	3 – 7 days (unintentional)	10 days	14 days – Removal (prior warning)
Penalty Guideline 5.34	Unavailability for Unscheduled Duty	N/A	Cancellation of LEAP	N/A

Congress of the United States
Washington, DC 20515

February 17, 2017

The Honorable Joseph P. Clancy
Director
The United States Secret Service
245 Murray Lane, SW
Washington, DC 20223

Dear Director Clancy:

We write today to formally request that you provide us with the details of any steps the United States Secret Service has taken to vet any person with access to President Trump's Mar-a-Lago Club (the Club).

On February 11, 2017, President Trump allegedly conducted a briefing on a North Korean missile test on a publicly accessible patio with the Prime Minister of Japan. In light of this event, we are deeply concerned that unauthorized individuals may gain access to critical national security information at the Mar-a-Lago Club, which the President refers to as the "Winter White House." This concern is further highlighted by the fact that Mr. Trump employs foreign nationals to staff the Club.

As a result, we request that you provide us with answers to the following questions:

1. Does the Secret Service run background checks on any and all persons, including members and their guests, who gain access to the Club in the same manner as White House guests are vetted?
2. Does the Secret Service conduct extensive vetting investigations on all personnel employed at the Club?
3. Does the Club employ foreign workers from Russia?
4. Does the Club employ foreign workers from any other country whose intelligence services may wish to gain access to American national security information?
5. Does any person with access to the club, including any foreign worker employed by the Club, have ties to any foreign intelligence service?
6. Is the Secret Service actively conducting counterintelligence operations to ensure that the Club is not compromised by a foreign intelligence service?
7. How much does it cost the Secret Service to conduct vetting investigations related to access to the Club?
8. Does the Club pay for or in any way reimburse the Secret Service for the costs associated with conducting vetting investigations of any person who gains access to the Club for purposes related to the business of the Club (i.e. not related to an official function of the United States government)?
9. If the Secret Service does not currently conduct these vetting investigations, why? And, how much would it cost the Secret Service to begin vetting the employees, members, guests, and any other person who gains entry to the Club?

We believe these questions are critical to protecting the national security of the United States and we respectfully request your personal attention to this matter to ensure a prompt response.

Sincerely,

Katherine Clark
Member of Congress

John Sarbanes
Member of Congress

Cedric L. Richmond
Member of Congress

Alcee L. Hastings
Member of Congress

Scott Peters
Member of Congress

Mark Pocan
Member of Congress

Steve Cohen
Member of Congress

Betty McCollum
Member of Congress

Barbara Lee
Member of Congress

Suzanne Bonamici
Member of Congress

Jamie Raskin
Member of Congress

David N. Cicilline
Member of Congress

David Price
Member of Congress

Marcy Kaptur
Member of Congress

Chellie Pingree
Member of Congress

Raja Krishnamoorthi
Member of Congress

Kathleen Rice
Member of Congress

Ann McLane Kuster
Member of Congress

James P. McGovern
Member of Congress

Nita M. Lowey
Member of Congress

Linda T. Sánchez
Member of Congress

Colleen Hanabusa
Member of Congress

Kathy Castor
Member of Congress

Seth Moulton
Member of Congress

Ted W. Lieu
Member of Congress

Carol Shea-Porter
Member of Congress

Lois Frankel
Member of Congress

Richard M. Nolan
Member of Congress

Sheila Jackson Lee
Member of Congress

Jerrold Nadler
Member of Congress

John Lewis
Member of Congress

Theodore E. Deutch
Member of Congress

Zoe Lofgren
Member of Congress

CC:
Deputy Director William J. Callahan
The United States Secret Service
245 Murray Lane, SW
Washington, DC 20223

United States Senate

WASHINGTON, DC 20510

March 3, 2017

Director Joseph Clancy
United States Secret Service
Office of Government and Public Affairs
245 Murray Lane
Washington, DC 20223

Dear Director Clancy:

We understand that you will be retiring at the end of this week and want to thank you for your leadership over the past three years. You helped steer the agency through a difficult time following highly-publicized security lapses and staffing shortfalls, and your willingness to return to public service to do so is greatly appreciated.

The Secret Service plays an unquestionably critical role in protecting our presidents and first families. We all share the utmost respect for the Secret Service's protective mission and for the dedicated officers that ensure the safety of our nation's elected leaders.

At the same time, recent events have raised questions about the scope and costs of security for the President and his family. As elected representatives entrusted with the oversight of taxpayer dollars, we write to request information from your agency about these costs.

In particular, news reports have detailed the costs of Secret Service protection for the President's adult sons while on foreign business trips benefiting the Trump Organization. Earlier this month, *The Washington Post* reported that a business trip to Uruguay by President Trump's adult son Eric cost taxpayers nearly $100,000 in hotels rooms alone for Secret Service and embassy staff.[1] This was not official business on behalf of the American people but, instead, promotion of the Trump Organization's business ventures. It was similarly reported earlier this month that adult sons Eric and Donald Jr. – ages 33 and 39, respectively – traveled with their Secret Service details to the United Arab Emirates to attend the opening

[1] Amy Brittain and Drew Harwell, "Eric Trump's business trip to Uruguay cost taxpayers $97,830 in hotel bills," Washington Post (Feb. 3, 2017).

RIF

of a Trump-branded golf resort,[2] and that Eric Trump also recently traveled to the Dominican Republic to evaluate a potential real-estate project.[3]

In addition to these trips to benefit the Trump Organization, other reports have focused on the costs of protecting President Trump, particularly when he stays at his own resort properties. While personal trips by the President are understandable, the President's three Mar-a-Lago trips since the inauguration have reportedly cost taxpayers $10 million dollars.[4]

This is not the first time that the legislative branch has expressed concern about presidential security costs. When President Obama took a three-day trip to Palm Beach, Florida, in 2013, some Members requested a Government Accountability Report on the cost of the trip. That trip cost $3.6 million, or roughly the same as *each one* of President Trump's trips to his Mar-A-Lago resort the past three weekends.[5]

It is the job of the Congress to provide meaningful oversight of these costs on behalf of the American people. We therefore ask that the agency provide the following information and documents:

1. A list of Trump family members being afforded Secret Service protection.

2. The cost, per day, for providing protection to each of President Trump's adult children (over age 25).

3. The full cost to the Secret Service of Eric Trump's trip to Uruguay.

4. The full cost to the Secret Service of Eric Trump's and Donald Trump Jr.'s trip to the United Arab Emirates.

5. A list of any other business trips taken by President Trump's adult children (over age 25) with Secret Service details and the full cost of those trips to the Secret Service.

---

[2] Jon Gambrell and Adam Schreck, "Trump sons open Dubai golf club as namesake now US president," Washington Post (Feb. 18, 2017).
[3] Joshua Partlow, "The Trump Organization may revive its failed Dominican resort project." Washington Post (Feb. 9, 2017).
[4] Drew Harwell, Amy Brittain, and Jonathan O'Connell, "Trump family's elaborate lifestyle is a 'logistical nightmare' — at taxpayer expense," Washington Post (Feb. 16, 2017).
[5] Jennifer Calfas, "Trump returning to Mar-a-Lago for third straight weekend," The Hill (Feb. 13, 2017).

RIF

6. The cost, per day, for providing Secret Service protection for President Trump's New York apartment.

7. The cost, per trip, for providing Secret Service protection for President Trump at the Mar-a-Lago resort in Florida.

8. All costs incurred by the Secret Service that are being paid to the Trump Organization or any business associated with the Trump Organization, and a breakdown of these costs that identifies the cost incurred (e.g., cost of leasing or overnight hotel stays), amounts paid, and the recipient of these payments.

Please arrange for the agency to provide responses to these questions by March 21, 2017. To the extent that the agency has concerns that answers to any of the questions might compromise security, please contact (b)(6);(b)(7)(C) of Ranking Member Feinstein's Committee staff at (b)(6);(b)(7)(C) so that we can discuss appropriate safeguards.

Again, thank you for your service to the country.

Sincerely,

Dianne Feinstein
United States Senator

Richard J. Durbin
United States Senator

Christopher A. Coons
United States Senator

Richard Blumenthal
United States Senator

cc: Charles E. Grassley, Chairman

United States Senate

WASHINGTON, DC 20510

March 6, 2017

William J. Callahan
Deputy Director
U.S. Secret Service
245 Murray Drive, SW, Building T5
Washington, DC 20223

Dear Deputy Director Callahan:

We write for information on the continuation and potential extension of the policy of providing public access to visitor logs for the White House complex, and to request you commit to similar measures for Mar-a-Lago and other locations where the President regularly conducts official business. This policy, adopted to cover records starting in September 2009, is responsible for making public the names of nearly six million visitors to the White House. As of the date of this letter, the Trump Administration has not indicated whether it will continue this policy.

It would be a significant setback to efforts to give the public insight into who influences the White House if this policy were to be discontinued or limited. Indeed, given the unique aspects of how President Trump has decided to conduct official business, we believe he needs to do even more just to meet the benchmark of transparency set by President Obama. President Trump has already taken four trips to his so-called "Winter White House" at his Mar-a-Lago estate in Florida, during which he conducted official business in full view of Mar-a-Lago members and their guests. During his transition, then President-elect Trump worked at the Trump Tower and the Trump National Golf Club in Bedminster, New Jersey, two locations that are also open to certain members of the public. Recently released audio of one post-election visit to Bedminster captured then President-elect Trump inviting members to "come around" as he interviewed people to serve in his Administration.

President Trump's conduct of official business at private property to which some members of the public have access appears to be unprecedented in recent times. While we appreciate that every President has the right to some privacy when not in the White House, this President has invited members of the public, who in many cases have paid significant amounts of money for access to him, to watch official business be conducted and has in some cases sought their advice during these breaks from Washington. To help us understand what steps this Administration is doing to maintain transparency and ensure proper vetting of individuals with access to the President and his staff, we request answers to the following questions:

- What determination, if any, has been made to continue making White House visitor logs from the Workers and Visitors Entry System (WAVES) and the Access Control Records system (ACR) available to the public?
- If there is a plan to continue to make these records available, will the policy differ from President Obama's? If so, how and why?

RIF

- Are the WAVES and the ACR systems being used for Mar-a-Lago? If not, what other steps are being taken to conduct background checks people who will be present during President Trump's trips to Mar-a-Lago?
- Is the Secret Service considering extending these systems, or any other security screenings, for Trump Tower, Bedminster, or other Trump properties at which the President may spend time conducting official businesses? If not, why not?
- If security screening systems are being put in place outside the White House, who will be responsible for collecting and maintaining these records, what information will be collected, and where and in what format it will be stored? Will information from those systems be made available to the public? If so, will that information be disclosed under the same conditions as White House visitor logs in the Obama Administration?

We request the courtesy of an answer to these questions no later than March 15, 2017.

Sincerely,

Sheldon Whitehouse
United States Senator

Ron Wyden
United States Senator

Jack Reed
United States Senator

Thomas R. Carper
United States Senator

Tom Udall
United States Senator

Kirsten E. Gillibrand
United States Senator

Richard Blumenthal
United States Senator

Chris Van Hollen
United States Senator

RIF

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

March 16, 2017

VIA ELECTRONIC TRANSMISSION

Acting Director William J. Callahan
United States Secret Service
Office of Governmental and Public Affairs
Washington, D.C. 20223

Dear Acting Director Callahan,

On March 3, 2017, colleagues on the Judiciary Committee wrote to then-Director Clancy to raise questions concerning the costs of providing protection for President Trump and certain family members. Specifically, they asked the cost, per day, to protect each of the adult children of President Trump. Other questions asked for the cost of providing protection to the Trump children when they traveled to attend family business matters. Finally, they asked for specific figures for maintaining protection at the Trump Tower in New York and each of the President's trips to Mar-a-Lago in Florida.

In order to provide the appropriate context for the answers to those questions and to fully understand your protective duties and their associated cost, please also provide the Committee with the following information no later than March 30, 2017:

1. Does the Secret Service normally provide protection to adult children of the President of the United States?

2. If yes, does the Secret Service suspend protection of the President or his immediate family members when they attend events relating to personal business not related to governmental matters?

3. It is well publicized that since leaving office in 2001, President Clinton and Secretary Clinton have combined to earn more than $153 million in paid speeches all over the world, including during her tenure as Secretary of State and in association with activities

of their private Clinton Foundation.[1] *The Washington Post* reports that since its inception in 1997, the Clinton Foundation has raised $2 billion in donations from individuals, corporations and foreign governments.[2] Please provide the full cost for providing protection to former President Clinton and Secretary Clinton and any other family members or requested protectees when they traveled to private speaking engagements or Clinton Foundation business from 2001 to present.

4. You previously received questions relating to the expenses the Secret Service has incurred as it relates to President Trump's visits to Mar-a-Lago. Please provide the full cost your agency has incurred since 2009 as it relates to providing protection for former President Obama and his family while they vacationed in both Martha's Vineyard, Massachusetts, and Oahu, Hawaii.

Thank you in advance for your cooperation with this request. Please number your responses according to their corresponding questions. If you have questions, please contact (b)(6);(b)(7)(C) of my Committee staff at (b)(6);(b)(7)(C)

Sincerely,

Charles E. Grassley
Chairman
Senate Committee on the Judiciary

cc:

The Honorable Diane Feinstein
Ranking Member
Senate Committee on the Judiciary

[1] Robert Yoon, *$153 Million in Bill and Hillary Clinton Speaking Fees, Documented*, CNN (Feb. 6, 2016), http://www.cnn.com/2016/02/05/politics/hillary-clinton-bill-clinton-paid-speeches.
[2] Matea Gold et al., *Inside the Clinton Donor Network*, WASH. POST (Nov. 19, 2015), https://www.washingtonpost.com/graphics/politics/clinton-money/.

MICHAEL T. McCAUL, TEXAS
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Fifteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

March 16, 2017

Mr. William J. Callahan
Acting Director
United States Secret Service
Department of Homeland Security
Washington, D.C. 20528

Dear Acting Director Callahan:

I am writing this letter to request additional information regarding the United States Secret Service's (USSS's) response to the recent security breach at White House on March 10, in which an individual was able to jump the fence and achieve close proximity to the White House itself. I would also like to inquire as to the value of measures taken by your agency to enhance the security effectiveness of the fence surrounding the White House complex.

On March 10, 2017, a suspect scaled an outer-perimeter fence on the White House complex's southeast side, near the Treasury Building, and was arrested without further incident by an officer in the agency's Uniformed Division (UD). According the U.S. Attorney's Office, the suspect was identified as Jonathan Tuan Tran, 26, of Milpitas, California. Court documents state that surveillance video shows Tran hiding behind a White House column. The arresting officer writes in the criminal complaint that he first observed Tran "walking close to the exterior wall of the White House mansion" and that Tran began heading toward the complex's south lawn upon being noticed. [1]

Since 2014, there have been a series of similar lapses in security at the White House. In October 2014, as a result of these troubling incidents, Former Secretary Jeh Johnson, requested an independent assessment of the security of the White House Complex (WHC). The assessment and recommendations were made by the United States Secret Service Protective Mission Panel. Pursuant to the Consolidated Appropriations Act of 2016, the Department of Homeland

[1] Joe Weber, "Suspected White House fence jumper charged with carrying 'dangerous weapon,' seen behind mansion column," March 11, 2017 < http://www.foxnews.com/politics/2017/03/11/suspected-white-house-fence-jumper-charged-with-carrying-dangerous-weapon-seen-behind-mansion-column.html>.

Security Office of Inspector General (DHS-OIG) reviewed the USSS's actions to address the recommendations of the Protective Mission Panel.[2] The DHS-OIG found that while the USSS has taken the Protective Mission Panel's nineteen recommendations seriously, including a recommendation to replace the outer fence of the White House, the USSS "still needed to determine the optimal arrangement...to promote streamlined communication, full information sharing, and inclusive decision making about the security of the WHC and the protection of the First Family".[3]

As a result of the numerous fence jumping incidents, in July 2015, the USSS installed an anti-climbing measure (steel spikes) on the top of the perimeter fencing of the White House; however, the temporary measures to deter individuals from climbing the fence appear to be ineffective. While I have complete confidence in the Secret Service's ability to execute its protective mission, I request a thorough investigation into this matter and responses to the following questions by March 31, 2017:

1. When and how was the suspect discovered on the WHC grounds?
2. Approximately how long was the suspect on the WHC grounds? How long was the suspect allegedly hiding behind a column?
3. What method did the suspect use to make his way over the outer perimeter fence?
4. How many Uniformed Division posts did the suspect proceed through while he was making his way to the south grounds?
5. Did the suspect attempt to use the pepper spray, reportedly found on him, when the arrest was being made?
6. Were tactical teams deployed when the breach of the WHC occurred?
7. Were the President and First Family evacuated to another location?
8. How close did the suspect get to the President and First Family?
9. Were the WHC grounds thoroughly searched after the incident? If so, was anything found as a result?
10. What was the total cost of installing the anti-climb feature on the WHC perimeter fencing?
11. Please describe in detail the security tests conducted on the anti-climbing steel spike installed on the outer perimeter fence, and the results of those tests.
12. What is the timeline for installation of the proposed outer perimeter security fence and gates?

The USSS is a premiere law enforcement agency with the most skilled agents and officers in the world. The agency's zero-fail mission is of the utmost importance to the national security of the United States. However, this recent incident continues to further harm morale within the agency. It is my intention to work with you and your staff on ways to improve morale and

[2] U.S. Department of Homeland Security Office of Inspector General (2016, November). *The Secret Service Has Taken Actions to Address the Recommendations of the Protective Mission Panel*. (Publication No. OIG-17-10)
[3] Ibid., pg. 13

enhance the overall standing of the Secret Service. With this in mind, I look forward to a continuing and open dialogue with you.

Thank you for your prompt attention to this matter. Should you have any questions please reach out to Ms. Krista Harvey on the Committee staff at (202) 226-8417.

Sincerely,

John Katko
Chairman
Subcommittee on Transportation
and Protective Security

JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
http://oversight.house.gov

March 17, 2017

Mr. William J. Callahan
Acting Director
U.S. Secret Service
950 H Street NW
Washington, D.C. 20223

Dear Mr. Callahan:

The Committee is investigating the March 10, 2017 security incident at the White House where the U.S. Secret Service (USSS) arrested an individual after he jumped the White House fence.[1] In an affidavit filed with the U.S. District Court for the District of Colombia, the arresting officer stated that the individual was carrying two cans of mace and "was walking close to the exterior wall of the White House mansion" and, at one point, hid "behind a White House pillar."[2]

The Committee has received allegations of additional information that was not included in the affidavit. According to those allegations, the individual may have triggered alarms the USSS ignored, may have moved around on the White House grounds undetected for a considerable amount of time, and may have attempted entry into the building. If true, these allegations raise questions about whether the agency's security protocols are adequate.

The Committee has longstanding concerns regarding repeated security incidents at USSS-protected facilities. The Committee's December 2015 bipartisan report found, "Over the last 10 years, there have been 143 security breaches and attempted security breaches at secured facilities which resulted in an arrest."[3]

To help the Committee assess whether these allegations are true, please provide a briefing at 5:00 p.m. on March 20, 2017. All video of the incident in question should be presented during that briefing. The Committee has reserved a secure space in the Office of House Security for the briefing.

---

[1] Azevedo Aff., Mar. 13, 2017.
[2] *Id.* ¶ 11.
[3] *H. Comm. on Oversight & Gov't Reform: United States Secret Service: An Agency in Crisis*, 114th Cong. (Dec. 9, 2015).

Additionally, please produce the following documents and information as soon as possible, but by no later than 5:00 p.m. on March 24, 2017:

N/A 1. All video of the White House grounds from the hours of 10:00 p.m. on March 10, 2017, to 1:00 a.m. on March 11, 2017;

OPO/RES 2. All logs of all activity at the Joint Operations Center from the hours of 10:00 p.m. on March 10, 2017, to 1:00 a.m. on March 11, 2017;

OPO/RES/CIO 3. All documents or communications related to any alarms on the White House grounds that may have been triggered from the hours of 10:00 p.m. on March 10, 2017, to 1:00 a.m. on March 11, 2017;

OPO/RES/CIO 4. All documents and communications referring or relating to the USSS' awareness of and response to this March 10, 2017, security incident; and

OPO/RES 5. All reviews of the incident and associated attachments.

To ensure the integrity of this or any other investigation, and that any potential future record requests can be fulfilled, please preserve all documents that can reasonably be anticipated to be subject to a request for production, specifically any video of the incident. Time is of the essence, as some videos, logs, or backup files may be transient or have short retention periods.

For the purposes of this request, "preserve" means taking reasonable steps to prevent the partial or full destruction, alteration, testing, deletion, shredding, incineration, wiping, relocation, migration, theft, or mutation of electronic records, as well as negligent or intentional handling that would make such records incomplete or inaccessible.

To ensure all responsive records are preserved, exercise reasonable efforts to identify and notify former employees and contractors, subcontractors and consultants who may have access to such electronic records that they are to be preserved. Further, exercise reasonable efforts to identify, recover, and preserve any electronic records which have been deleted or marked for deletion but are still recoverable. If it is the routine practice of the company to delete any records, either halt such practices or arrange for the preservation of complete and accurate duplicates or copies of such records, suitable for production, if requested. Electronic records should be construed broadly and includes videos, log files, messages and any other document or communication stored electronically.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format. An attachment to this letter provides additional information about responding to the Committee's request. Please note that Committee Rule 16(b) requires counsel representing an individual or entity before the Committee or any of its

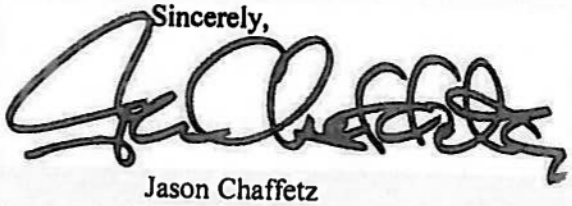
RIF

subcommittees, whether in connection with a request, subpoena, or testimony, promptly submit the attached notice of appearance to the Committee.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and has broad authority to investigate "any matter" at "any time" under House Rule X.

Please contact (b)(6);(b)(7)(C) of the majority staff at (b)(6);(b)(7)(C) with any questions about this request. Thank you for your attention to this matter.

Sincerely,



Jason Chaffetz
Chairman

Enclosure

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.

2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.

3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.

4. Documents produced in electronic format should also be organized, identified, and indexed electronically.

5. Electronic document productions should be prepared according to the following standards:

   (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.

   (b) Document numbers in the load file should match document Bates numbers and TIF file names.

   (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.

   (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document;

   BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH, PAGECOUNT,CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE, SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM, CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE, DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD, INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION, BEGATTACH.

6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.

8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.

9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.

10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.

11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.

12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.

13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.

14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.

15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.

16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.

17. All documents shall be Bates-stamped sequentially and produced sequentially.

18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.

19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term "document" means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.

2. The term "communication" means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.

3. The terms "and" and "or" shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.

4. The terms "person" or "persons" mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

RIF

5. The term "identify," when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.

6. The term "referring or relating," with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.

7. The term "employee" means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
115TH CONGRESS

NOTICE OF APPEARANCE OF COUNSEL

Counsel submitting: _____

Bar number: _____ **State/District of admission:** _____

Attorney for: _____

Address: _____

Telephone: (_____) _____ - _____

Pursuant to Rule 16 of the Committee Rules, notice is hereby given of the entry of the undersigned as counsel for _____ **in (select one):**

- (●) **All matters before the Committee**
- ( ) **The following matters (describe the scope of representation):**

_____

_____

All further notice and copies of papers and other material relevant to this action should be directed to and served upon:

Attorney's name: _____

Attorney's email address: _____

Firm name (where applicable): _____

Complete Mailing Address: _____

_____

I agree to notify the Committee within 1 business day of any change in representation.

_____ _____

Signature of Attorney **Date**

RIF

United States Senate

WASHINGTON, DC 20510

March 21, 2017

The Honorable William J. Callahan
Deputy Director
United States Secret Service
245 Murray Lane
Washington, DC 20223

Dear Deputy Director Callahan:

We are writing in furtherance of our investigation relating to President Trump's claim that President Obama wiretapped Trump Tower. Please answer the following questions by April 4, 2017:

1. Did the Secret Service conduct any security sweeps of Trump Tower for surveillance equipment between January 1, 2015 and today?
2. If the Secret Service did conduct any such security sweep, was any surveillance equipment found? What were the results of any such security sweep?
3. Did the Secret Service attempt to determine the source of any surveillance equipment discovered at Trump Tower? If so, what was the source?
4. Did the Secret Service attempt to determine for how long any such surveillance equipment was operational at Trump Tower? If so, for how long was such surveillance equipment operational?
5. What was the type of information or communication captured by any such surveillance equipment? Audio? Visual? Other?

We have written Deputy Attorney General Boente and FBI Director Comey previously for copies of court orders and warrant applications related to any wiretapping of Trump Tower. As with the FBI and DOJ's criminal division, the Subcommittee on Crime and Terrorism, of which we are the Chairman and Ranking Member, has oversight of the Secret Service.

We look forward to your response.

Sincerely,

Lindsey O. Graham
United States Senator

Sheldon Whitehouse
United States Senator

RIF

DAVE BRAT
7TH DISTRICT, VIRGINIA

COMMITTEE ON
THE BUDGET

COMMITTEE ON EDUCATION
AND THE WORKFORCE

COMMITTEE ON
SMALL BUSINESS

Congress of the United States
House of Representatives
Washington, DC 20515–4607

330 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-2815
(202) 225-0011 (F)

4201 DOMINION BOULEVARD
SUITE 110
GLEN ALLEN, VA 23060
(804) 747-4073
(804) 747-5308 (F)

9104 COURTHOUSE ROAD
ROOM 249
(MAILING ADDRESS:
9104 COURTHOUSE ROAD
P.O. BOX 99)
SPOTSYLVANIA, VA 22553
(540) 507-7216
(540) 507-7019 (F)

January 4, 2017

Mr. Chris Stanley
Deputy Assistant Director
Office of Congressional Affairs
U S Secret Service
245 Murray Drive, SW, Building T5
Washington, DC 20223-0001

Dear Mr. Stanley :

One of my constituents contacted me regarding a problem that they have encountered and I am hopeful that you may be of assistance. I have enclosed all of the information that we have received on this particular case for your review.

If you or a member of your staff would look into this matter and provide any information that might be useful, I would be most grateful. Should you require any additional information, please do not hesitate to contact me or my District Representative, (b)(6);(b)(7)(C), in my Glen Allen Office at (b)(6);(b)(7)(C) or (b)(6);(b)(7)(C)

In reply, I would appreciate if you would direct correspondence to my District Office by mail to 4201 Dominion Blvd, Suite 110, Glen Allen, VA 23060, by fax to 804-747-5308, or by email to (b)(6);(b)(7)(C)

Sincerely,

Dave Brat
Member of Congress

DB/ZW

CONGRESSMAN DAVE BRAT
7th DISTRICT OF VIRGINIA

CONSTITUENT RELEASE FOR SERVICE
PRIVACY ACT RELEASE

In accordance with Title 5, section 522 (a), of the United States Code, (the Privacy Act), I hereby authorize Congressman Dave Brat to request assistance on my behalf as he may deem necessary.

Please Print:

Name (b)(6);(b)(7)(C)

Address (b)(6);(b)(7)(C)

Phone Number (b)(6);(b)(7)(C)

Email Address

Date of Birth (b)(6);(b)(7)(C)

Social Security Number

Name of Agency

Claim Number

Nature of Problem:

(b)(6);(b)(7)(C)

Date: 12/20/2016

Signature (b)(6);(b)(7)(C)

JOHN P. SARBANES
3RD DISTRICT, MARYLAND

COMMITTEE ON
ENERGY AND COMMERCE

2444 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4016
FAX: (202) 225-9219

Congress of the United States
House of Representatives
Washington, DC 20515–2003

www.sarbanes.house.gov

January 27, 2017

Mr. Chris Stanley
Deputy Assistant Director
United States Secret Service
245 Murray Drive, Sw, Building T5
Washington, DC 20223

Dear Mr. Stanley:

I have been contacted by my constituent (b)(6);(b)(7)(C) (b)(6);(b)(7)(C) (b)(6);(b)(7)(C) (b)(6);(b)(7)(C) (b)(6);(b)(7)(C) (b)(6);(b)(7)(C) (b)(6);(b)(7)(C) I have attached a copy of the signed privacy release from the constituent as well as a copy of the correspondence provided to me describing the situation.

I respectfully request your staff look into this matter and provide my office with a response so that I may reply to my constituent appropriately. Please direct all correspondence to (b)(6);(b)(7)(C) on (b)(6);(b)(7)(C) fax (410)832-8898 Thank you very much.

Sincerely,

John Sarbanes
Member of Congress

JS\fh

600 BALTIMORE AVENUE
SUITE 303
TOWSON, MD 21204
(410) 832-8890
FAX: (410) 832-8898

44 CALVERT STREET
SUITE 349
ANNAPOLIS, MD 21401
(410) 295-1679
FAX: (410) 295-1682

CONGRESSMAN JOHN P. SARBANES

Constituent Service Request Form

Name: (b)(6);(b)(7)(C)

Address

Home Phone: (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

Federal Agency Involved: U.S. Secret Service/DHS

ID# or Case#

Email: (b)(6);(b)(7)(C)

Brief Description of the Problem*: (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

*Please attach an explanation of your situation and copies of pertinent documents, letters, etc.

Disclosure Authorization

I am aware that Public Law 93-579 (the Privacy Act of 1974) prohibits the release of personal information contained in my records without my permission.

I authorize United States Secret Service/Dept Homeland Security (Federal Agency) to pro (b)(6);(b)(7)(C) claim to Congressman John P. Sarbanes and his staff.

Signat Date: 1/18/2017

Print

I hereby authorize Congressman John P. Sarbanes and his staff to discuss the results of this inquiry on my behalf with the following individual:

Signature: Date:

Please return this completed form to:
U. S. Representative John P. Sarbanes
600 Baltimore Avenue, Suite 303 · Towson, Maryland 21204
Telephone: (410) 832-8890 · Fax: (410) 832-8898

(b)(6);(b)(7)(C)

January 18, 2017

The Honorable John Sarbanes

Dear Representative Sarbanes:

(b)(6);(b)(7)(C)

I am writing you to ask that you help ascertain why the U.S. Secret Service has failed to take systematic and proactive measures to take corresponding corrective action to respond to a claim of damage caused by their negligent operations.

(b)(6);(b)(7)(C)

I appreciate your help and ask that you please send me a response letting me know if you are able to ascertain why the U.S. Secret Service is avoiding their responsibility to compensate me for the actual expenses incurred by their negligent operations. I ask that the U.S Secret Service be compelled to take prompt action to resolve this claim fairly and quickly.

Thank you for your time and considering my request. I am attaching copies of the claim to this letter for your reference.

(b)(6);(b)(7)(C)

CONGRESSMAN FRANK PALLONE, JR.
6TH DISTRICT, NEW JERSEY
67/69 CHURCH STREET
New Brunswick, New Jersey 08901
(732) 249-8892 Phone *** (732) 249-1335 Fax

WWW.HOUSE.GOV/PALLONE

FACSIMILE TRANSMITTAL SHEET

TO: Congressional Liaison

FAX NUMBER: (202) 406 - 5740

FROM: (b)(6);(b)(7)(C)

DATE: 2/2/17

RE: (b)(6);(b)(7)(C)

TOTAL NO. OF PAGES, INCLUDING COVER: 4

☐ URGENT ☑ FOR REVIEW ☐ PLEASE COMMENT ☑ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

Please see the attached inquiry. I look forward to your response.

Best,

(b)(6);(b)(7)(C)

RANKING MEMBER
COMMITTEE ON
ENERGY AND COMMERCE

FRANK PALLONE, JR.
6TH DISTRICT, NEW JERSEY

REPLY TO:
☐ 237 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-3006
(202) 225-4671

☐ 504 BROADWAY
LONG BRANCH, NJ 07740
(732) 571-1140

✓ 67/69 CHURCH STREET
NEW BRUNSWICK, NJ 08901
(732) 246-8892

TOLL-FREE NUMBER:
(888) 423-1140

pallone.house.gov

Congress of the United States
House of Representatives
Washington, DC 20515–3006

February 1, 2017

Mr. Chris Stanley
Deputy Assistant Director
Office of Congressional Affairs
United States Secret Service
245 Murray Drive, SW, Building T5
Washington, DC 20223

RE: (b)(6);(b)(7)(C)

Dear Mr. Stanley:

My constituent, (b)(6);(b)(7)(C) has recently contacted me. (b)(6);(b)(7)(C) has asked that I contact your agency on his behalf.

Attached please find a copy of my constituent's letter pertaining to a polygraph examination for his application to the Uniform Division of the United States Secret Service.

In advance, I would like to thank you for taking the time to review his concerns. Please feel free to contact (b)(6);(b)(7)(C) directly should you decide to take any action on this matter.

Sincerely,

Frank Pallone Jr.

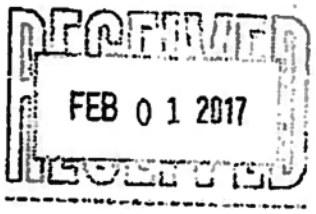
FRANK PALLONE, JR.
Member of Congress

FP/jd
Enclosure

Thursday, January 26, 2017

(b)(6);(b)(7)(C)

The Honorable Frank Pallone
United States House of Representatives
67/69 Church Street
New Brunswick, NJ 08901-1242



Dear Mr. Pallone:

(b)(6);(b)(7)(C)

ELIJAH E. CUMMINGS
7TH DISTRICT, MARYLAND

RANKING MEMBER, COMMITTEE ON
OVERSIGHT AND GOVERNMENT REFORM

RANKING MEMBER,
SELECT COMMITTEE ON BENGHAZI

COMMITTEE ON
TRANSPORTATION AND INFRASTRUCTURE
SUBCOMMITTEE ON COAST
GUARD AND MARITIME TRANSPORTATION
SUBCOMMITTEE ON
RAILROADS, PIPELINES, AND HAZARDOUS
MATERIALS

Congress of the United States
House of Representatives
Washington, DC 20515

☐ 2230 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-2007
(202) 225-4741
FAX: (202) 225-3178

DISTRICT OFFICES:

☒ 1010 PARK AVENUE
SUITE 105
BALTIMORE, MD 21201-5037
(410) 685-9199
FAX: (410) 685-9399

☐ 754 FREDERICK ROAD
CATONSVILLE, MD 21228-4504
(410) 719-8777
FAX: (410) 455-0110

☐ 8267 MAIN STREET
ROOM 102
ELLICOTT CITY, MD 21043-9903
(410) 465-8259
FAX: (410) 465-8740

www.cummings.house.gov

January 17, 2017

Chris Stanley
Deputy Assistant Director
Office of Congressional Affairs
U.S. Secret Service
245 Murray Drive, SW, Building T5
Washington, DC 20223

Dear Mr. Stanley:

(b)(6);(b)(7)(C)

Any assistance that you can provide to my constituent would be greatly appreciated. Please review this matter and forward your reply to my office at 1010 Park Avenue, Suite 105, Baltimore, Maryland 21201. Should you require further information or assistance, please do not hesitate to contact me or my Special Assistant, Ms. (b)(6);(b)(7)(C) at (b)(6);(b)(7)(C)

Sincerely,

Elijah E. Cummings
Member of Congress

EEC/cl

Enclosures

Congressman Elijah E. Cummings
Request For Assistance

Washington Office:	District Offices:		
2230 Rayburn H.O.B. Washington, D.C. 20515 (202) 225-4741 office (202) 225-3178 fax	1010 Park Avenue, Ste. 105 Baltimore, MD 21201 (410) 685-9199 office (410) 685-9399 fax	754 Frederick Road Catonsville, MD 21228 (410) 719-8777 office (410) 455-0110 fax	8267 Main Street, Rm 102 Ellicott City, MD 21043 (410) 465-8259 office (410) 465-8740 fax
☐	☑	☐	☐

Staff Contact: Ms. (b)(6);(b)(7)(C) Office: 1010 Park Ave.

Instructions:
Please complete the following information and return this form to the office listed above.

Name: (b)(6);(b)(7)(C)

Address:

City, State

Phone (H): None

SS#: (b)(6);(b)(7)(C)

Date of Birth: (b)(6);(b)(7)(C)

Email Address: (b)(6);(b)(7)(C)

Phone (C): (b)(6);(b)(7)(C)

NOTICE: THE PRIVACY ACT OF 1974 REQUIRES THAT WRITTEN CONSENT BE OBTAINED FROM THE CONSTITUENT BEFORE INFORMATION CAN BE OBTAINED FROM RECORDS WITH A GOVERNMENT AGENCY. IN ORDER THAT I MIGHT ACT ON YOUR BEHALF, I WOULD APPRECIATE YOUR SIGNING AND RETURNING THE FOLLOWING STATEMENT TO ME. IF YOU ARE INQUIRING ON BEHALF OF SOMEONE OTHER THAN YOURSELF, THAT INDIVIDUAL WILL NEED TO SIGN THIS PRIVACY RELEASE FORM.

Dear Congressman Cummings:

This is to authorize you to obtain and provide information as you may deem necessary pertaining to my request for your assistance.

(b)(6);(b)(7)(C)
SIGNATURE

1/3/2017
DATE

Provide the Nature of the Problem/Agency Involved:

Please see the attached document detailing my issue.

Rev. 082015 fa

(b)(6);(b)(7)(C) **(GPA)**

From: Higbee, Donovan (b)(6);(b)(7)(C)
Sent: Monday, February 13, 2017 3:42 PM
To: (b)(6);(b)(7)(C) (GPA)
Subject: Rep. Mimi Walters - (b)(6);(b)(7)(C)
Attachments: (b)(6);(b)(7)(C) 2-13-17.pdf

Good afternoon (b)(6);(b)(7)(C)

Thank you for taking my call earlier. I am writing today on behalf of U.S. Representative Mimi Walters' constituent (b)(6);(

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

For your reference, I have enclosed (b)(6);(b)(7)(privacy release form, which includes more details about his application process. Thank you in advance for your assistance, and please let me know if you have any questions.

Best regards,

Donovan Higbee

District Representative
U.S. Representative Mimi Walters (CA-45)
3333 Michelson Drive, Suite 230 | Irvine, California 92612
Office: 949.263.8703 | Fax: 949.263.8704 | donovan.higbee@mail.house.gov
Website | Facebook | Twitter | Instagram | Youtube

Sign-up for Rep. Mimi Walter's Newsletter today!

Post-it® Fax Note 7671	Date 2/1/17	# of pages ▶ 2
To Office of Mimi Walters	From (b)(6);(b)(7)(C)	
Co./Dept. U.S. House of Rep.	Co.	
Phone # 949-263-8703	Phone (b)(6);(b)(7)(C)	
Fax # 949-263-8704	Fax #	

Congresswoman Mimi Walters

Please print, sign and mail/fax to our office.

Name (b)(6);(b)(7)(C)

Date: 2017-02-01

Agency Involved: UNITED STATES SECRET SERVICE

Numbers Identifying Case (VA claim, Alien number, tax ID, etc.): NONE

Branch of Service (If Applicable): N/A

Military Rank (If Applicable) (b)(6);(b)(7)(C)

Date of Birth: (b)(6);(b)(7)(C)

Street Address: (b)(6);(b)(7)(C)

City, State, Zip Code: (b)(6);(b)(7)(C)

Telephone # (b)(6);(b)(7)(C)

Email Address (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE
Washington, D.C. 20223

March 22, 2017

The Honorable Mimi Walters
Member of Congress
3333 Michelson Drive, Suite 230
Irvine, California 92612

Dear Mrs. Walters:

Thank you for your inquiry on behalf of your constituent, (b)(6);(b)(7)(C) who applied for a position within the U.S Secret Service as a Medical Officer.

(b)(6);(b)(7)(C)

If I can be of assistance with this or any other matter in the future, please do not hesitate to contact me.

Sincerely,

R. Christopher Stanley
Deputy Assistant Director

OFFICE OF CONGRESSMAN GLENN THOMPSON

3555 Benner Pike, Suite 101
Bellefonte, PA 16823

(814) 353-0215 Fax (814) 353-0218

To: Mr. Chris Stanley x5676
From: (b)(6);(b)(7)(C)
Date: 2/18/17
Fax Number: (202) 406-5740
Subject: (b)(6);(b)(7)(C)

FAXED

Total Pages (including cover sheet): 5

Comments: Could you please look into this matter at your earliest convenience?

Thank you,

AD

GLENN "GT" THOMPSON
6TH DISTRICT, PENNSYLVANIA

124 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-3806
(202) 226-5121
(202) 226-5790 (FAX)

http://thompson.house.gov

AGRICULTURE
Chairman, Subcommittee on Conservation, Energy, and Forestry

EDUCATION & THE WORKFORCE

NATURAL RESOURCES

Congress of the United States
House of Representatives

February 18, 2017

Mr. Chris Stanley
Deputy Assistant Director
Office of Congressional Affairs
U.S. Secret Service
245 Murray Drive, SW, Building T5
Washington, DC 20223-0001

Dear Mr. Stanley:

(b)(6);(b)(7)(C)

Enclosed please find a copy of the recent correspondence that I have received pertaining to the case. I would very much appreciate your review of this matter. Kindly respond with a report of your findings to my Bellefonte District Office at 3555 Benner Pike, Suite 101, Bellefonte, PA 16823, telephone (814) 353-0215 or fax (814) 353-0218.

Thank you, in advance, for your assistance with this case inquiry.

Sincerely,

G.T. Thompson

Glenn "GT" Thompson
Member of Congress

GT/ad

FEB 17 2017

Case Information and Privacy Act Release Form

PAS

Information Release

The provisions of the Federal Privacy Law of 1974, Public Law 93-579 require that I receive your written authorization to allow the various federal agencies I contact on your behalf to provide me a detailed reply.

I hereby request the assistance of the Office of Congressman Glenn "GT" Thompson to resolve the matter described below. I authorize Congressman Glenn "GT" Thompson and his staff to receive any information from the federal agencies that is required to provide this assistance.

Please concisely outline the problem and state your proposed resolution:
(If more space is required, please continue on page 2)

(b)(6);(b)(7)(C)

Return Form To: Congressman Glenn Thompson, 3555 Benner Pike, Suite 101, Bellefonte, PA 16823
(814) 353-0215 or fax (814) 353-0218

Thank you for allowing me to assist your with your federal issue. As a Member of Congress, my staff and I will do our very best to assist you. Although we cannot force a federal agency to act in your favor, we can be an advocate and encourage the federal authorities to give your case full consideration under all applicable agency rules. Further, please note that House Rules do not allow me to intervene in legal court matters.

Full Name: (b)(6);(b)(7)(C) **Date of Birth:** (b)(6);(b)(7)(C)

Address (b)(6);(b)(7)(C)

City: (b)(6);(b)(7)(C) **State:** (b)(6);(b)(7)(C) **Zip:** (b)(6);(b)(7)(C)

Day Telephone: (b)(6);(b)(7)(C) **Cell Phone:**

E-Mail Address:

Federal Agency Involved: DHS - Secret Service

Case Number: (b)(6);(b)(7)(C)
(Social Security #, Alien #, Receipt #, Tax ID #, VA Claim #)

SIGNATURE: (b)(6);(b)(7)(C) **DATE:** 2-10-2017

Secret Service
17 N 2nd Street #1701
Harrisburg, Pa. 17101

M&T Bank
283 Hoggon Boulevard, Mill Hall, PA 17751

RIF

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE

Washington, D.C. 20223

February 28, 2017

The Honorable Glenn Thompson
Member of Congress
3555 Benner Pike, Suite 101
Bellefonte, Pennsylvania 16825

Dear Mr. Thompson:

Thank you for your inquiry on behalf of your constituent, (b)(6);(b)(7)(C) regarding the status of a counterfeit currency investigation.

(b)(6);(b)(7)(C);(b)(7)(E)

I hope this information is helpful. If I can be of further assistance with this or any other matter in the future, please do not hesitate to contact my office.

Sincerely,

Thomas C. Edwards
Special Agent in Charge

(b)(6);(b)(7)(C) **(GPA)**

From: (b)(6);(b)(7)(C) GPA)
Sent: Tuesday, February 21, 2017 12:44 PM
To: (b)(6);(b)(7)(C) (GPA)
Subject: FW: (b)(6);(b)(7)(C)
Attachments: (b)(6);(b)(7)(C) Priv Release Form.pdf

From: (b)(6);(b)(7)(C) [mailto (b)(6);(b)(7)(C)
Sent: Friday, February 17, 2017 2:58 PM
To: (b)(6);(b)(7)(C)
Subject: (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

Thanks,

(b)(6);(b)(7)(C)
Field Representative
Representative Keith Rothfus, PA-12
Tel: 412-837-1361 Fax: 412-593-2022
(b)(6);(b)(7)(C)
Rothfus.house.gov

KEITH J. ROTHFUS
PENNSYLVANIA'S TWELFTH DISTRICT

COMMITTEE ON
FINANCIAL SERVICES

Congress of the United States
House of Representatives

This form authorizes the release of information in my records to Congressman Keith J. Rothfus.

Name: (b)(6);(b)(7)(C)

Address: (b)(6);(b)(7)(C)

Phone: (b)(6);(b)(7)(C)

Email Address: (b)(6);(b)(7)(C)

Social Security Number: (b)(6);(b)(7)(C)

Date of Birth: (b)(6);(b)(7)(C)

Other Applicable Numbers (i.e. Receipt Number, Veteran ID): _____

Federal Agency Involved: U.S Secret Service

Tax Years/Years in Question (for IRS concerns): _____

Signature: (b)(6);(b)(7)(C)

Date: 12 JAN 2017

PLEASE PROVIDE DETAILS ABOUT YOUR CONCERN.

(b)(6);(b)(7)(C)

BEAVER OFFICE
650 CORPORATION STREET, SUITE 304
BEAVER, PA 15009
PHONE: 724-351-1696
FAX: 412-393-5022

JOHNSTOWN OFFICE
110 FRANKLIN STREET, SUITE 150
JOHNSTOWN, PA 15901
PHONE: 814-619-3659
FAX: 412-393-5022

ROSS TOWNSHIP OFFICE
6000 HERRON BOULEVARD, SUITE 104
PITTSBURGH, PA 15237
PHONE: 412-837-1361
FAX: 412-393-5022

WASHINGTON D.C. OFFICE
1005 LONGWORTH HOB
WASHINGTON, D.C. 20515
PHONE: 202-225-2065
FAX: 202-225-3759

ROTHFUS.HOUSE.GOV

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE

Washington, D.C. 20223

February 22, 2017

The Honorable Keith J. Rothfus
Member of Congress
6000 Babcock Boulevard, Suite 104
Pittsburgh, Pennsylvania 15237

Dear Mr. (b)(6);(b)(

Thank you for your inquiry on behalf of your constituent, (b)(6);(b)(7)(C)

A representative from the Secret Service's Office of Human Resources, Administrative, Professional, Technical Staffing Branch, spoke with (b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

(b)(6);(b)(7)(C)

The enclosed information was shared with (b)(6);(b)(7)(C) however, should he have any additional questions we recommend that he contact the Secret Service Liaison Division, Freedom of Information Act/Privacy Act Program, at (202) 406-6370.

I hope this information was helpful. If you should need further assistance with this or any other matter in the future, please do not hesitate to contact my office.

Sincerely,

Thomas C. Edwards
Special Agent in Charge

Enclosure

Freedom of Information & Privacy Act
Making a Request

Making a FOIA Request

The Department of Homeland Security (6 CFR Chapter 1 and Part 5) requires:

1. A request for records shall be made in writing.
2. You must describe the records that you seek in enough detail to enable the agency to locate them with a reasonable amount of effort. Whenever possible, your request should include specific information about each record sought, such as the date, title or name, author, recipient and subject matter of the record.
3. If you are making a request for records about another individual, you must provide either a written authorization signed by that individual permitting disclosure of those records to you or proof that the individual is deceased (for example, a copy of a death certificate or an obituary).
4. If you make a FOIA request, it shall be considered a firm commitment by you to pay all applicable fees charged under Sec. 5.11 up to $25, unless you seek a waiver of fees. In making a FOIA request, please indicate whether you are willing to pay for the request or desire a waiver. When making a request, you may specify a willingness to pay a greater or lesser amount. If you are seeking a waiver of fees, you must provide a justification for your fee waiver request in accordance with the requirements of Sec. 5.11(k).

Where to File a Request

Request should be submitted to the following address:

Communications Center (FOIA/PA)
245 Murray Lane, Building T-5
Washington, D.C. 20223

Fax: 202-406-5586
Email: FOIA@usss.dhs.gov

Making a Privacy Act Request

If you are making a request for records about yourself, you must provide either a notarized statement or a statement signed under penalty of perjury stating that you are the person that you say you are. You may fulfill this requirement by:

- having your signature on your request letter witnessed by a notary; or
- including the following statement immediately above the signature on your request letter: "I declare under penalty of perjury that the foregoing is true and correct. Executed on [date]."

If you request information about yourself and do not follow one of these procedures, your request cannot be processed. This requirement helps ensure that private information about you will not be disclosed to anyone else.

(b)(6);(b)(7)(C) **(GPA)**

From: Office of Representative Susan W. Brooks (imailagent) <IN05SBIMA@mail.house.gov>
Sent: Tuesday, February 21, 2017 2:29 PM
To: (b)(6);(b)(7)(C) (GPA)
Cc: (b)(6);(b)(7)(C)
Subject: Congressional Inquiry (b)(6);(b)(7)(C)
Attachments: (b)(6);(b)(7)(C) PR.pdf; IQFormatFile.txt

Dear Mr. Stanley,

My constituent, (b)(6);(b)(7)(C) has contacted my office concerning the status of his reconsideration request for a medical denial to his application for special agent.

Enclosed is a signed authorization form and copies of correspondence I have received from my constituent.

I would appreciate it if you would review this matter and provide me with any information that may be helpful to my constituent. Please direct your response to (b)(6);(b)(7)(C) in my Anderson, Indiana office.

I am grateful for any assistance you may be able to provide in this case.

Sincerely,

Susan W. Brooks
Member of Congress

Please do not reply to this email. The mailbox is unattended.
To share your thoughts please visit my webpage.

Susan W. Brooks
Fifth District, Indiana

COMMITTEES:

Energy and Commerce

Select Committee on Benghazi

Ethics

Congress of
the United States
House of Representatives
Washington, DC 20515-1402

D.C. Office:
1505 Longworth House Office Building
Washington, DC 20515
(202) 225-2276
Fax: (202) 225-0016

Carmel Office:
11611 North Meridian Street, Ste. 415
Carmel, IN 46032
(317) 848-0201
Fax: (317) 846-7306

Anderson Office:
120 East 8th Street, Ste. 101
Anderson, IN 46016
(765) 640-5115
Fax: (765) 640-5116

Authorization in Accordance with the 1974 Privacy Act

Name: (b)(6);(b)(7)(C) Date of Birth: (b)(6);(b)(7)(C)

Address: (b)(6);(b)(7)(C)

City: (b)(6);(b)(7)(C) State: (b)(6);(b)(7)(C) Zip: (b)(6);(b)(7)(C)

Home Phone: (b)(6);(b)(7)(C) Work Phone: _____ Email: (b)(6);(b)(7)(C)

Social Security #: (b)(6);(b)(7)(C) Receipt or Other Case #: (b)(6);(b)(7)(C)

Attorney: _____ Attorney Phone#: _____

Have you contacted another elected official about this matter? Yes (No) (circle one) If so, who? _____

Please describe the specific information you are requesting or the exact nature of the problem you are experiencing. Send copies of any relevant information (DO NOT SEND ORIGINALS). Please include what agency you are working with and indicate if you have a representative working for you. Use extra paper if necessary.

(b)(6);(b)(7)(C)

THE PRIVACY ACT OF 1974 PROHIBITS THE GOVERNMENT FROM REVEALING ANY INFORMATION FROM PERSONAL FILES OF INDIVIDUALS WITHOUT THE EXPRESS PERMISSION OF THE PERSON INVOLVED. DISCLOSURE OF PERSONAL RECORDS TO A MEMBER OF CONGRESS WHO IS ACTING ON BEHALF OF THE CONSTITUENT IS PROHIBITED, UNLESS THE INDIVIDUAL TO WHOM THE RECORD PERTAINS HAS CONSENTED.

I, the undersigned, hereby authorize the office of U.S. Representative Susan W. Brooks to receive information in my file pertinent to her inquiry on my behalf.

SIGNATURE: (b)(6);(b)(7)(C) Date: 02/16/2017

☐ I would like to receive e-newsletters and other important information from Congresswoman Brooks

TIM KAINE
VIRGINIA

COMMITTEE ON
ARMED SERVICES

COMMITTEE ON
FOREIGN RELATIONS

COMMITTEE ON
THE BUDGET

COMMITTEE ON
HEALTH, EDUCATION, LABOR,
AND PENSIONS

WASHINGTON OFFICE:

WASHINGTON, DC 20510-4607
(202) 224-4024

United States Senate

WASHINGTON, DC 20510-4607

February 15, 2017

U.S. Department of Homeland Security
301 7th St SE # 3621
Washington, DC 20003

Dear Sir or Madam:

Enclosed is a privacy release and letter from my constituent, (b)(6);(b)(7)(C) in reference to an issue he has encountered involving U.S. Secret Service and Department of Homeland Security.

(b)(6);(b)(7)(C)
(b)(6);(b)(7)(C)
(b)(6);(b)(7)(C) Your immediate attention and assistance with the concerns expressed in this case would be greatly appreciated.

I would also appreciate being provided a response that I may forward to (b)(6);(b)(7)(explaining the status of case. Please respond to my Director of Casework, (b)(6);(b)(7)(C) at: 919 East Main Street, Suite 970, Richmond, VA 23219. You may also reach (b)(6);(b) by phone at (b)(6);(b)(7)(C) or by e-mail at:
(b)(6);(b)(7)(C)

Thank you for your assistance to my constituent.

Sincerely,

Tim Kaine

United States Senate
WASHINGTON, DC 20510-4801

Our team may be able to answer basic questions over the phone; however, if your situation requires further research, a specialist may open a case and initiate a congressional inquiry on your behalf. The Privacy Act of 1974 requires congressional offices to obtain written permission from an individual before a federal agency can release any specific information to the Senator. If you would like to request help, please complete the following Privacy Release Authorization and return it to our Richmond office as directed below. Family members, friends or other interested parties generally may not authorize the release of information on your behalf. As soon as I receive this form, I will be pleased to do everything I can to provide assistance to you.

Timothy M. Kaine
United States Senate

PRIVACY RELEASE AUTHORIZATION

Federal Agency Involved*: USSS

Briefly describe your situation: *(use additional page if needed)*

I hereby request the assistance of the Office of Senator Tim Kaine to resolve the matter described above and authorize Senator Kaine or his staff to receive any information that may be needed to provide this assistance. The information I have provided in true and accurate to the best of my knowledge and belief. The assistance I have requested from Senator Kaine is in no way an attempt to violate any federal, state or local law.

(b)(6);(b)(7)(C)

Full Name *(please print)* & Date of Birth*

(b)(6);(b)(7)(C)

Email address *(if available)*

(b)(6);(b)(7)(C)

Signature

11/1/2016

Date

(b)(6);(b)(7)(C)

Phone Number *(including area code)*

Account/Claim Number*

**Required Information*

While we are happy to work on your behalf, we typically avoid opening a constituent case that is currently being handled by another Senator or House member as this may cause delays in resolution. Do you currently have an open case for the matter described above with another U. S. Senator or Representative?

✓ Yes ____ No If yes, please provide the members name Rep Barbara Comstock

RETURN COMPLETED FORM TO:

Senator Tim Kaine
ATTN: Constituent Services
919 E. Main Street, 970
Richmond, VA 23219

OR

Fax (804) 771-8313
ATTN: Constituent Services

Thank you for taking time to read about my situation and any assistance you can provide.

(b)(6);(b)(7)(C) **(Kaine)**

From: (b)(6);(b)(7)(C)
Sent: Wednesday, November 30, 2016 9:51 AM
To: (b)(6);(b)(7)(C) Kaine)
Cc: (b)(6);(b)(7)(C) (Kaine)
Subject: Update

Sir,

(b)(6);(b)(7)(C)

Respectfully,

(b)(6);(b)(7)(C)

DEBBIE WASSERMAN SCHULTZ
23RD DISTRICT, FLORIDA

CHIEF DEPUTY WHIP

COMMITTEES:
COMMITTEE ON APPROPRIATIONS
RANKING MEMBER
SUBCOMMITTEE ON MILITARY CONSTRUCTION, VETERANS AFFAIRS, AND RELATED AGENCIES
SUBCOMMITTEE ON ENERGY AND WATER DEVELOPMENT, AND RELATED AGENCIES
SUBCOMMITTEE ON LEGISLATIVE BRANCH
COMMITTEE ON THE BUDGET
STEERING AND POLICY COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515-0923

WASHINGTON OFFICE:
1114 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-0923
(202) 225-7931
(202) 225-2052 (FAX)

DISTRICT OFFICES:
777 SAWGRASS CORPORATE PARKWAY
SUNRISE, FL 33325
(954) 845-1179
(954) 845-0396 (FAX)

19200 WEST COUNTRY CLUB DRIVE
AVENTURA, FL 33180
(305) 936-5724
(305) 932-9664 (FAX)

FAX COVER SHEET

To: CONGRESSIONAL UNIT

From:

Debbie Wasserman Schultz
Member of Congress

Lori Green
District Director
(lori.green@mail.house.gov)

Vivian Piereschi
Deputy District Director
(vivian.piereschi@mail.house.gov)

Laurie Flink
Deputy District Director
(laurie.flink@mail.house.gov)

Bettyanne Gallagher
Director Constituent Services/Casework
(bettyanne.gallagher@mail.house.gov)

Michael Liquerman
Outreach Coordinator/Press
(michael.liquerman@mail.house.gov)

Phillip Jerez
District Outreach Coordinator
(phillip.jerez@mail.house.gov)

Phones: Broward: (954) 845-1179
Dade: (305) 936-5724

Fax: (954) 845-0396
Fax: (305) 932-9664

Date: 3/3/17

Total pages faxed: 9

Fax #: 202-406-5740

Notes:

RIF

CONGRESSWOMAN DEBBIE WASSERMAN SCHULTZ
777 SAWGRASS CORPORATE PARKWAY
SUNRISE, FL 33325
Phones: Broward (954) 845-1179 Dade: (305) 936-5724 Fax: (954) 845-0396

****

PRIVACY RELEASE FORM

(The Privacy Act of 1974 [Public Law 93-579] prevents agencies from releasing information about you or anyone else without the person's written consent. Therefore, if you would like for me to intervene with a federal agency on your behalf, I need your signature on this waiver.) Please print

Full Name: (b)(6);(b)(7)(C)

Address: (b)(6);(b)(7)(C)

Home Phone: _____ **Work Phone:** (b)(6);(b)(7)(C)

Cell Phone: (b)(6);(b)(7)(C) **Social Security # :** _____
(ONLY if applicable)

Fax: _____ **E-mail*:** (b)(6);(b)(7)(C)

(*Please note: By providing your e-mail, you are subscribing to my newsletter.)

Explanation of problem with federal agency:

I wrote a appeal in regards to being considered for Secret Service Agent. I have not receive any correspondence to my appeal.

I hereby authorize the appropriate federal government agency to release any and all information pertaining to me and my case to Congresswoman Debbie Wasserman Schultz or any of her staff.

Signature: (b)(6);(b)(7)(C) **Date:** 2/28/17

For Immigration, Embassy, or Passport Inquiries:

Name of subject: _____ **D.O.B.** _____

Place of birth: _____ **Port of Entry** _____

Alien Registration #: _____ **Date of arrival to U.S.** _____

Forms submitted to CIS, corresponding receipt numbers, and date submitted:

Original Letter Sent

April 8, 2016

SA Support Branch (b)(6);(b)(7)(C)

245 Murray Lane,S.W. Building T-5

Washington, DC 20223

Dear Brach Chief Washington:

(b)(6);(b)(7)(C)

February 28, 2017

SA Support Branch (b)(6);(b)(7)(C)

245 Murray Lane,S.W. Building T-5

Washington, DC 20223

Dear Brach Chief Washington:

(b)(6);(b)(7)(C)

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE
Washington, D.C. 20223

March 20, 2017

The Honorable Christopher H. Smith
Member of Congress
112 Village Center Drive, Second Floor
Freehold, New Jersey 07728

Dear Mr. Smith:

Thank you for your inquiry concerning a claim for damages arising from an auto accident involving your constituent (b)(6);(b)(7)(C) and an employee of the U.S. Secret Service (Secret Service).

Please be advised that the Secret Service was in contact with (b)(6);(b)(7)(C) on March 15, 2017, and is working to resolve her claim.

I hope this information is useful. If I can be of assistance with this or any other matter in the future, please do not hesitate to contact me.

Sincerely,

Thomas C. Edwards
Special Agent in Charge

From:

03/16/2017 08:34 #936 P.001/004

Congressman Warren Davidson

U.S. House of Representatives

www.davidson.house.gov

☐ 1414 Longworth H.O.B, Washington, DC 20515 - 202-225-6205 - 202-225-0704 fax

☒ 8857 Cincinnati-Dayton Rd., #102, West Chester, OH 45069 - 513-779-5400 - 513-779-5401 fax

☐ 12 S. Plum Street, Troy, OH 45373 - 937-339-1524 - 937-339-1878 fax

☐ 76 E. High St., 3rd Floor, Springfield, OH 45502 - 937 322 1120 - 937-327-2515 fax

FAX COVER SHEET

Date: March 16, 2017

To: US. Secret Service Congressional Liaison

Fax: 202-406-5740 **Phone:** _____

From: (b)(6);(b)(7)(C)

Message: (b)(6);(b)(7)(C) & delayed background clearance renewal, - See Waiver

Total Pages: 4

If there is a problem with the transmission of this fax, please call 513-779-5400.

Rep. Warren Davidson

MAR 06 2017

Butler County Prosecutor Office

PRIVACY ACT RELEASE FORM

PLEASE PRINT CLEARLY

Mr. Mrs. Ms. (circle one) **Full Name:** (b)(6);(b)(7)(C) **Nick Name:**

Address of Residence: (b)(6);(b)(7)(C)

City/State/Zip: (b)(6);(b)(7)(C) **County** (b)(6);(b)(7)(C)

Phone #: Home (b)(6);(b)(7)(C) **Work ( )** **Other ( )**

Email Address: (b)(6);(b)(7)(C)

☐ Check here to receive email updates from Congressman Warren Davidson

Please send completed form to: Congressman Warren Davidson

Residents of Butler, Preble, Darke & Mercer Counties: (b)(6);(b)(7)(C)

[illegible] Cincinnati Bell Inn Road, Suite
West Chester, Ohio 45069

7[illegible] Main Street
[illegible], OH 45[illegible]

Due to the provisions of the Privacy Act of 1974 (Title 5, Section 552A of the United States Code):
Permission in writing is required before making an inquiry on your behalf. Completing and signing this form

Rep. Warren Davidson

MAR 06 2017

Butler County District Office

PRIVACY ACT RELEASE FORM

PLEASE PRINT CLEARLY

Mr./Mrs./Ms. (circle one) **Full Name:** (b)(6);(b)(7)(C) **Nick Name:** _____

Address of Residence: (b)(6);(b)(7)(C)

City/State/Zip: (b)(6);(b)(7)(C) **County** (b)(6);(b)(7)(C)

Phone #: Home (b)(6);(b)(7)(C) **Work (___)** _____ **Other (___)** _____

Email Address: (b)(6);(b)(7)(C)

☑ **Check here to receive e-mail updates from Congressman Warren Davidson.**

Please send completed forms to: Congressman Warren Davidson

Residents of Butler, Preble, Darke & Mercer Counties:
8857 Cincinnati-Dayton Road, #102
West Chester, Ohio 45069

Residents of Clark and Miami Counties:
12 South Plum Street
Troy, Ohio 45373

Due to the provisions of the Privacy Act of 1974 (Title 5, Section 552A of the United States Code):
Permission in writing is required before making an inquiry on your behalf. Completing and signing this form authorizes Rep. Warren Davidson and the staff of the 8th Congressional District to make inquiries to the appropriate officials on your behalf, and the release of information to the Congressman or his staff. This permission is on-going until revoked in writing or the stated issue is resolved.

To begin your inquiry, provide all pertinent information related to your case/claim:

Federal Agency Involved: U.S. SECRET SERVICE

Social Security Number: (b)(6);(b)(7)(C) **Date Of Birth:** (b)(6);(b)(7)(C)

Military ID#: _____ **Veteran's Claim #:** _____

Military Branch, Rank & Unit: _____

Alien #: A _____ **CIS/DOS Receipt #:** _____

Immigration – Petitioner's Name: _____

Beneficiary's Name: _____

Other Numbers Identifying your claim: _____

Please briefly describe your situation and the action, result, or information you desire. Use the back of this sheet, or attach a separate page, if necessary. Be sure to provide any necessary documentation.

SEE ATTACHED PAGES

SIGNATURE (b)(6);(b)(7)(C) **DATE:** 3/5/17

09/19/2016

A Facsimile from the Office of Congressman Dave Reichert WA-08
22605 SE 56th St, Suite 130
Issaquah, WA 98029
Phone: 425.677.7414
Fax: 425.270.3589

To: CONGRESSIONAL LIAISON

Date: 20 MARCH 2017

Fax Number: (202) 406-5740

From:

- ☐ **Dave Reichert, Congressman**
- ☐ **Sue Foy, District Director**
- ☐ **Tom Young, Deputy District Director**
- (b)(6);(b)(7)(C) **Senior Outreach Manager/Grants Manager**
- (b)(6);(b)(7)(C) **, Senior Outreach Manager**
- (b)(6);(b)(7)(C) **Constituent Services Liaison**
- (b)(6);(b)(7)(C) **, Central WA Constituent Services Liaison**

Pages (includes cover sheet):

RE: (b)(6);(b)(7)(C)

District Congressional Office
22605 SE 56th St, Suite 130
Issaquah, WA 98029
Toll Free: 877-920-9208
Phone: 425-677-7414
Fax: 425-270-3589

Congressman David G. Reichert
Member of Congress
Washington's 8th Congressional District

www.reichert.house.gov

Casework Authorization Form

Please print legibly

Full Name:	(b)(6);(b)(7)(C)	**Date of Birth:**	(b)(6);(b)(7)(C)
...on behalf of: *(if applicable)*		**Social Security #:**	
Relationship: *(if applicable)*		**Home Phone #:**	
Mobile Phone #:	(b)(6);(b)(7)(C)	**Work Phone #:**	
E-mail:		**Fax #:**	
Mailing Address:		**Physical Address:** *(if different)*	
City:	(b)(6);(b)(7)(C)	**State:**	(b)(6);(b)(7)(C)
Claim/File #: *(LIN # / Case # / Alien # / File #, etc.)*	N/A - THE SECRET SERVICE STATES THEY ARE SELF INSURED	**Zip Code:**	(b)(6);(b)(7)(C)
Federal Agency(ies) involved:	U.S. SECRET SERVICE		

Constituent Permission

Please Note: The Privacy Act requires that you authorize access to your private records and authorize this office to release information [illegible] our

Desired Resolution: (b)(6);(b)(7)(C)

Please

(b)(6);(b)(7)(C)

I hereby request the assistance of the Office of United States Representative David G. Reichert in resolving the matter described in this document. I authorize and/or release any information needed to provide assistance.

Signature: (b)(6);(b)(7)(C) **Date:** 3/16/17

Please print and fax or mail to our District Office along with copies of any other documentation that you think might be helpful to us when making an inquiry on your behalf. Please understand that you are responsible for all your original documents or copies, and must retain these for your records. We are not permitted to accept gifts for any services you receive. Your signature above is acknowledgement of this policy. We look forward to assisting you. Thank you.